Project no. 826278

SERUMS

Research & Innovation Action (RIA)
SECURING MEDICAL DATA IN SMART-PATIENT HEALTHCARE SYSTEMS

Refined Requirements Analysis and Success Metrics
D7.4

Due date of deliverable: 31st March 2020

Start date of project: 1st January 2019

Type: Deliverable
WP number: WP7

Responsible Institution: ZMC
Editor and editor's address: Mestrum Mark (m.mestrum@zuyderland.nl)
Partners Contributing: ZMC, USTAN, ACC, IBM, SOPRA, SCCH, UCY, FCRB

Approved by:
Reviewers: Marios Belk (UCY)
Euan Blackledge (SOPRA)

Version 1.1

Project co-founded by the European Commission within the Horizon H2020 Programme		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Release History

Release No.	Date	Author(s)	Release Description/Changes made
V0.1	07/05/2019	Mestrum Mark (ZMC)	Updates on Introduction section
V0.2	13/07/2019	Mestrum Mark (ZMC), Ivo Buil (ZMC), Leon van de Weem (ZMC), Marios Belk (UCY), Elias Athanasopoulos (UCY), Andreas Pitsillides (UCY), Christos Feidas (UCY), Euan Blackledge (Sopra), Michael Vinov (IBM), Wanting Huang (ACC), Michael Roßbory (SCCH), Santiago Iriso (FCRB), David Vidal (FCRB), Thomas Given-Wilson (UCL)	Updates on the SERUMS technologies technical requirements and on the expected impacts and success indicators
V0.3	11/09/2019	Mestrum Mark (ZMC), Ivo Buil (ZMC), Leon van de Weem (ZMC), Marios Belk (UCY), Elias Athanasopoulos (UCY), Christos Feidas (UCY), Andreas Pitsillides (UCY), Euan Blackledge (Sopra), Michael Vinov (IBM), Wanting Huang (ACC), Michael Roßbory (SCCH), Santiago Iriso (FCRB), David Vidal (FCRB)	Updates on SERUMS expected impacts and success indicators
V0.4	06/11/2019	Mestrum Mark (ZMC), Ivo Buil (ZMC), Leon van de Weem (ZMC), Marios Belk (UCY), Elias Athanasopoulos (UCY), Christos Feidas (UCY), Andreas Pitsillides (UCY), Euan Blackledge (Sopra), Michael Vinov (IBM), Wanting Huang (ACC), Michael Roßbory (SCCH), Santiago Iriso (FCRB), David Vidal (FCRB), Thomas Given-Wilson (UCL), Eduard Baranov (UCL)	Updates on the KPIs measurements for the evaluation of SERUMS success indicators

V0.5	17/12/2019	Mestrum Mark (ZMC), Ivo Buil (ZMC), Leon van de Weem (ZMC), Marios Belk (UCY), Elias Athanasopoulos (UCY), Christos Feidas (UCY), Andreas Pitsillides (UCY), Euan Blackledge (Sopra), Michael Vinov (IBM), Wanting Huang (ACC), Michael Roßbory (SCCH), Santiago Iriso (FCRB), David Vidal (FCRB), Thomas Given-Wilson (UCL), Eduard Baranov (UCL)	Updates on the SERUMS Technologies Technical Requirements and objectives
V0.7	17/12/2019	Mestrum Mark (ZMC), Ivo Buil (ZMC), Leon van de Weem (ZMC), Marios Belk (UCY), Elias Athanasopoulos (UCY), Christos Feidas (UCY), Andreas Pitsillides (UCY), Euan Blackledge (Sopra), Michael Vinov (IBM), Bram Elshof (ACC), Wanting Huang (ACC), Michael Roßbory (SCCH), Santiago Iriso (FCRB), David Vidal (FCRB) Thomas Given-Wilson (UCL), Eduard Baranov (UCL)	Updates on the SERUMS expected impacts and success indicators
V0.8	31/01/2020	Mestrum Mark (ZMC), Ivo Buil (ZMC), Leon van de Weem (ZMC), Marios Belk (UCY), Elias Athanasopoulos (UCY), Christos Feidas (UCY), Andreas Pitsillides (UCY), Euan Blackledge (Sopra), Michael Vinov (IBM), Bram Elshof (ACC), Wanting Huang (ACC), Michael Roßbory (SCCH), Santiago Iriso (FCRB), David Vidal (FCRB), Thomas Given-Wilson (UCL), Eduard Baranov (UCL)	Updates on the SERUMS expected impacts and success indicators

V0.9	20/03/2020	Mestrum Mark (ZMC), Ivo Buil (ZMC), Leon van de Weem (ZMC), Marios Belk (UCY), Elias Athanasopoulos (UCY), Christos Feidas (UCY), Andreas Pitsillides (UCY), Euan Blackledge (Sopra), Michael Vinov (IBM), Bram Elshof (ACC), Wanting Huang (ACC), Michael Roßbory (SCCH), Santiago Iriso (FCRB), David Vidal (FCRB), Thomas Given-Wilson (UCL), Eduard Baranov (UCL)	Updates on the SERUMS technologies technical requirements, on the expected impacts and success indicators and on the KPIs measurements for the evaluation of SERUMS success indicators.
V1.0	25/03/2020	Mestrum Mark (ZMC)	Final version of D7.4 provided to the deliverable reviewers for final review
V1.1	31/03/2020	Mestrum Mark (ZMC), Ivo Buil (ZMC), Leon van de Weem (ZMC), Marios Belk (UCY), Elias Athanasopoulos (UCY), Christos Feidas (UCY), Andreas Pitsillides (UCY), Euan Blackledge (Sopra), Michael Vinov (IBM), Bram Elshof (ACC), Wanting Huang (ACC), Michael Roßbory (SCCH), Santiago Iriso (FCRB), David Vidal (FCRB), Thomas Given-Wilson (UCL), Eduard Baranov (UCL)	Finalization of D7.4 based on the comments received from the reviewers and release of D7.4.

SERUMS Consortium

Partner 1	**University of St Andrews**
Contact Person	Name: Juliana Bowles Email: jkfb@st-andrews.ac.uk
Partner 2	**Zuyderland Medisch Centrum**
Contact Person	Name: Mark Mestrum Email: m.mestrum@zuyderland.nl
Partner 3	**Accenture B.V.**
Contact Person	Name: Bram Elshof, Wanting Huang Email: bram.elshof@accenture.com, wanting.huang@accenture.com
Partner 4	**IBM Israel Science & Technology Ltd.**
Contact Person	Name: Michael Vinov Email: vinov@il.ibm.com
Partner 5	**Sopra-Steria**
Contact Person	Name: Andre Vermeulen Email: andreas.vermeulen@soprasteria.com
Partner 6	**Université Catholique de Louvain**
Contact Person	Name: Axel Legay Email: axel.legay@uclouvian.be
Partner 7	**Software Competence Centre Hagenberg**
Contact Person	Name: Michael Rossbory Email: michael.rossbory@scch.at
Partner 8	**University of Cyprus**
Contact Person	Andreas Pitsillides Email: andreas.pitsillides@ucy.ac.cy
Partner 9	**Fundació Clínic per a la Recerca Biomèdica**
Contact Person	Name: Santiago Iriso Email: siriso@clinic.cat

Table of Contents

Executive Summary

In order to achieve high quality healthcare provision, it is increasingly important to collect highly confidential and personal medical data (obtained from a variety of sources including personal medical devices) and share this through a variety of means (including public networks and other systems) whose security cannot be implicitly trusted. Thus, there is a strong and urgent demand to deliver better, more efficient and more effective healthcare solutions that can achieve excellent patient-centric healthcare provision, while also complying with increasingly strict regulations on the use and sharing of patient data.

Towards this end, SERUMS aims to increase efficiency while also ensuring the increased safety of patients and the privacy of sensitive health data using innovative techniques that will increase resilience to cyber-attacks and promote trust in the safe and secure operation of the system. In order to meet this challenge, SERUMS will develop and implement innovative methods, tools and technologies addressing the need for cybersecurity in hospitals including remote care and home-care settings. Through these developments, SERUMS project expects to achieve significant impact in each area that has been identified in the SU-TDS-02-2018 call, providing significantly more secure smart health care provision, with significantly reduced potential for data breaches, and significantly improved patient trust and safety.

This deliverable defines the technical challenges/requirements that the different tools/technologies comprised in the coherent SERUMS system will need to satisfy. The identified requirements will be fed into each of the technical work packages, forming a foundation for the design and implementation of the associated methods and tools. Also, it defines the success indicators that will be used for measuring SERUMS progress and specific impact in terms of: **i)** Improved security of Health and Care services, data and infrastructures; **ii)** Less risk of data privacy breaches caused by cyber-attacks; and **iii)** Increased patient trust and safety. In particular, considering the use cases described in D7.3, this deliverable (D7.4) provides clear definitions of the Key Performance Indicators (KPIs), along with their corresponding metrics, as well as the Baseline and the Trial measurements that will be used for measuring the success indicators.

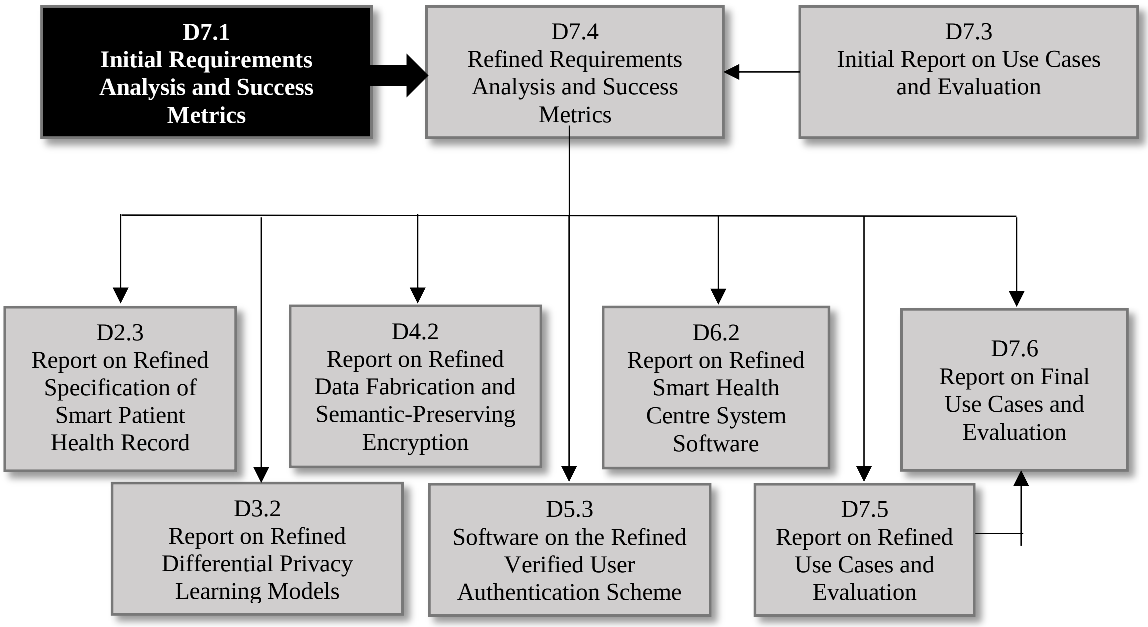
1 Introduction

1.1 Role of the Deliverable

The role of this deliverable is twofold. First, it aims to define the requirements of the SERUMS project as a whole. More specifically, based on the Description of Work and the identified use cases in D7.3, this document defines the main technical challenges/requirements that the different tools/technologies, methods and techniques comprised in the coherent SERUMS solution will need to satisfy. These are then forwarded to the technical work packages, so as to be considered for the design and implementation of the respective tools/technologies and methods. Second, it aims to define a detailed description of the success indicators for the overall expected impacts. In particular, it provides clear definitions of the Key Performance Indicators (KPIs), along with their corresponding metrics, as well as the Baseline and the Trial measurements that will be used for measuring the success indicators.

1.2 Relationship to other SERUMS Deliverables

The relationship of D7.4 (that builds on D7.1) with the other SERUMS deliverables is provided in the figure below.


D7.1
Initial Requirements Analysis and Success Metrics
D7.4
Refined Requirements Analysis and Success Metrics
D7.3
Initial Report on Use Cases and Evaluation
D2.3
Report on Refined Specification of Smart Patient Health Record
D4.2
Report on Refined Data Fabrication and Semantic-Preserving Encryption
D6.2
Report on Refined Smart Health Centre System Software
D7.6
Report on Final Use Cases and Evaluation
D3.2
Report on Refined Differential Privacy Learning Models
D5.3
Software on the Refined Verified User Authentication Scheme
D7.5
Report on Refined Use Cases and Evaluation

1.3 Structure of this Document

Following the current introductory chapter, the rest of the document is structured as follows. Chapter 2 describes the SERUMS project technical objectives and requirements. Also, the main technical and functional challenges as well as main objectives that must be addressed by the SERUMS Technologies are described. Chapter 3 provides clear definitions of the Key Performance Indicators (KPIs), along with their corresponding metrics, as well as the Baseline and the Trial measurements, as well as the formulas that will be used for measuring the success indicators. Chapter 4 provides the ethical challenges that should be addressed in the SERUMS project. Finally, Chapter 5 provides some conclusions.

2 SERUMS Technical Objectives and Requirements

SERUMS project aims to increase efficiency while also ensuring the increased safety of patients and the privacy of sensitive health data. SERUMS will achieve this by implementing innovative methods, tools and technologies addressing the need for cybersecurity in hospitals including remote care and home-care settings. Towards this end, the SERUMS project technical objectives and requirements, the main technical and functional challenges as well as the main objectives that must be addressed by the SERUMS Technologies, are provided below.

2.1 SERUMS Key Challenges

The overall vision is to realise an integrated and patient-centric distributed Smart healthcare System, which enhances the quality of patient care by taking advantage of recent advances in monitoring and communication, while simultaneously providing trust and confidence that the system respects patient privacy and data protection concerns. Provisioning such a secure, trustworthy, but efficient and effective patient-centric smart healthcare system presents a number of key challenges:

- **Challenge 1:** Patients must have a high degree of trust both that the smart healthcare system operates as intended, and that their privacy is fully protected.
- **Challenge 2:** The smart healthcare system must provide a high level of transparency in its operation, yet must not leak information.
- **Challenge 3:** The smart healthcare system must work efficiently as a whole in order to maximise the quality of patient care, yet must simultaneously provide high levels of security and support high expectations of privacy and anonymity.
- **Challenge 4:** The patient must have full control of their data, as required by the GDPR and other legislation, yet the data must be provided in a timely fashion to medical practitioners and specialists.
- **Challenge 5:** In order to support emergency medicine or other forms of trans-border medical treatment, the smart healthcare system must comply with multiple, possibly conflicting, legislative frameworks.

2.2 SERUMS Overall Technical Requirements

The challenges identified above require a new and radical approach that tackles issues of security, data protection, privacy and trust in a coherent and holistic way that promotes effective medical treatment, including across systems, and across local/national borders. In order for the SERUMS vision to be achieved, a number of technical requirements must be met.

Authentication	
1	All agents must be properly authenticated to the system.
2	Only authorized agents can have access to data;
3	Agents can have access only to the data that they have been explicitly granted permission to access.
4	Only the patient and other properly authorized representatives can grant permission to access the patient record and other personal/sensitive data.

Establishing Trust	
1	The smart healthcare system must be fully compliant with the provisions of the GDPR and other relevant national and international legislation.
2	Information must not inadvertently leaked during communication, both in terms of data, and in

	terms of communication patterns.
3	All accesses to and changes to data must be logged immutable, and be available for inspection
4	It must not be possible to repudiate any data history.
5	The patients must be always able to access their own personal health record, see all of the items in the record, and manage access to that record.

Enabling Efficiency	
1	The security measures must be proportionate and do not impose excessive computational or network cost, especially on edge devices.
2	Data must be transmitted and stored efficiently.
3	Data must be available when required by the patient, the system, the medical practitioners, etc.
4	Data analytics must be able to take advantage of the heterogeneity and real-time information that is offered by the holistic smart healthcare system.

Managing Data	
1	Data that is collected from a variety of sources must be stored and processed in a consistent way.
2	Data must be available when required.
3	Suitable granular access must be provided to data records.
4	Unstructured and semi-structured data must be indexed in a way that makes it easily accessible for future use.
5	Full records are maintained of changes to and accesses to data items.

2.3 SERUMS Technologies Technical Requirements

This section identifies the main technical and functional challenges as well as main objectives that must be addressed by the SERUMS Technologies. More specifically, by considering the overall technical challenges of the SERUMS system as well as the use cases described in D7.3, the main technical and functional requirements and objectives of each Technology comprised in the coherent SERUMS system have been identified and described. These are then forwarded into each of the Technical work packages, forming a foundation for the design and implementation of the associated methods and tools. Also these are considered in Chapter 3 for the definition of the Key Performance Indicators (KPIs), along with their corresponding metrics, as well as the Baseline and the Trial measurements that will be used for measuring the success indicators.

2.3.1 Personalized User Authentication (PUA) Tool

Personalized User Authentication, namely FlexPass, is a flexible and multi-factor user authentication system that combines knowledge-based user authentication types (picture-based and text-based), along with token-based user authentication utilizing push notifications on smartphones and smartwatches. With regards to the picture-based authentication type, FlexPass is based on a novel retrospective-based image content delivery approach [10][11] that provides images tailored to each user’s prior daily life activities and experiences to make them more memorable and secure. In addition, in case users would like to use textual passwords, they can also create a textual password (in the form of a secret passphrase) which they can use to flexibly switch between their picture password to login.

PUA Technical Challenges	
1	Build and maintain appropriate user models that will describe in a holistic way what constitutes the user’s physical, technological and interaction context in which computation takes place.
2	Building mechanisms for quantifying the security and memorability of user-selected passwords.

3	Implement decision making and adaptive policies for providing best-fit recommendations with regards to the authentication type, image content, image complexity, etc. to the end-users.

PUA objectives in the SERUMS System	**Relevant KPIs and metrics**
Improve password guessability	This is associated with KPI 1.1 (Guessability) that will be measured using the following metrics: key space, theoretical entropy, practical entropy, guess number, textual password complexity, raphical password complexity, push notification accuracy.
Improve protection against password leaks (through social engineering)	This is associated with KPI 1.2 (Password leaks - through social engineering) that will be measured using the following metrics: memory time, shoulder surfing.
Improve password usability	This is associated with KPI 3.1 (Perceived Usability) that will be measured using the following metrics: perceived usability, time to create password, time to login, number of failed attempts to create password, number of failed attempts to login.
Improve password memorability	This is associated with KPI 3.2 (Perceived Memorability) that will be measured using the following metrics: perceived memorability, memory time, time to login, number of failed attempts to login, number of password resets.
Improve perceived security	This is associated with KPI 3.3 (Perceived Security) that will be measured using the following metrics: perceived security.
Build users' trust towards the user authentication system	This is associated with KPI 3.4 (Perceived Trust) that will be measured using the following metrics: perceived trust.

2.3.2 Smart Patient Record (SPR)

The Smart Patient Record is a central access point to all the relevant information about a single patient, including both static data such as the patient name, age and address and dynamic data, such as the data about treatments, prescriptions and insurance. Over the course of the SERUMS project, the aim is to define the format of the smart patient records for each of the use cases that will be considered. Also, if feasible, a common format for all of the use cases will be defined that will capture the similarities between them while allowing also for representation of the case-specific data.

Smart Patient Record Technical Challenges	
1	Develop a machine readable (JSON or similar) format of the Smart Patient Records that will give enough information to the data fabrication mechanisms to generate synthetic but realistic patient data.
2	Develop a suitable representation for the remote data which may reside in the different administrative unit compared to the central patient record, and which might need to be accessed over untrusted networks.
3	Capture the similarities between different use cases into an universal Smart Patient Record format.
4	Implement different views for the patient records (e.g., for patients, GPs, specialists, insurers), respecting privacy regulations and specific access rights.
5	Develop storage and access methods for Smart Patient Records that will ensure compliance to the privacy and security regulations while also allowing the novel authentication, data cloaking

	etc. methods to be implemented over them.
6	Develop machine-learning models to pre-process the unstructured data, extract the meta-data from it and incorporate it into the patient records.

SPR objectives in the SERUMS System	**Relevant KPIs and metrics**
Create a secure platform to create and store the Smart Patient Health Record (SPHR) before transmission	This is associated with KPI 1.3: System Vulnerability. The current level of security, such as operating system, programming language, and firewall status will be measured by a graded questionnaire.
Reduce the risk of data breaches associated with the current access controls	This is associated with KPI 2.2: Data Breaches. The access levels of various types of staff will be measured by a graded questionnaire.
Reduce the risk of data breaches associated with the current method of sharing data with external parties	This is associated with KPI 2.2: Data Breaches. The current method of physical transportation and the risk associated with the loss of the data will be measured by a graded questionnaire.
Improve the patients' trust in the system by improving security and reducing the risk of data breaches	This is associated with KPI 3.5: Patient Trust. A short graded questionnaire will be given to patients to measure their trust in the current system, and compare these results to their trust in the demo system when the changes have been explained to them

2.3.3 Data Fabrication Platform (DFP)

The IBM Data Fabrication Platform (DFP) is a web-based central platform for generating high-quality data for testing, development, and training. The platform provides a consistent and organisational wide methodology for creating test data. The methodology used is termed “rule guided fabrication”. In rule guided fabrication, the data and metadata logic is extracted from the underlying real data or its description and is modelled using rules that the platform provides.

Once a user requests the generation of a certain amount of data into a set of test databases or test files, the platform internally ensures that the generated data satisfies the modelled rules as well as the internal data consistency requirements.

The platform is capable of: generating data from scratch; inflating existing databases or files; moving existing data; and transforming data from previously existing resources, such as old test databases, old test files or even production data. In essence, the platform provides a comprehensive and hybrid solution that is capable of creating a mixture of synthetic and real data according to user requirements.

DFP Technical challenges	
1	Support the Smart Patient Record (SPR) format defined in the project and its single data-field and cross data-field dependencies and fabrication rules.
2	Develop a support for mixed file/database fabrication mode.
3	Enhance DFP advanced data analytics to enable automatic creation of data fabrication rules from the underling SPR metadata and data properties to enable automatic fabrication rules creation.

DFP objectives in the SERUMS System	**Relevant KPIs and metrics**
Support the Smart Patient Record (SPR) format and fabrication of realistic synthetic data to improve testing of SERUMS's healthcare system and thus reduce its	Not associated with any KPIs. Its role is supportive for the SPR.

vulnerability.	

2.3.4 Credential Hardening (CH)

Authentication involves storing some user credentials in a server and use them for user validation in future logins. These credentials are stored in databases, and they can be, for instance, cryptographic hashes of salted passwords. Upon a database breach, weak passwords can be cracked (even in the case where a strong cryptographic hash function is used). CH will deliver new techniques for storing credentials using cryptographic techniques so that, once the stored data is leaked, then it becomes useless to the attacker.

CH Technical challenges	
1	Store authentication credentials in a vulnerable server that might eventually get leaked.
2	Protect users when the server's data (that includes credentials) is leaked.
3	Employ techniques based on cryptography that are easy to deploy and do not degrade the server's overall performance.

CH objectives in the SERUMS System	**Relevant KPIs and metrics**
Improve password cracking resistance	This is associated with KPI 2.1 (Password Cracking Resistance) that will be measured using the following metrics: password cracking resistance rate.

2.3.5 Privacy-preserving Data Analytics (PDA)

The data on which a machine learning or a data analytics algorithm operates might be owned by more than one party and a party may be unwilling to share its real data. The reason being that an algorithm's output may result in a leakage of private or sensitive information regarding the data. Differential privacy is a standard framework to quantify the degree to which the data privacy of each individual in the dataset is preserved while releasing the algorithm output. A common method to preserve the differential privacy is of adding a random noise to the output of a query on the dataset. Despite the fact that random noise adding mechanism has been widely used for privacy-preserving machine learning, there remain still two challenges:

PDA Technical challenges	
1	There is no standard approach to efficiently design a general noise adding mechanism, independent of the machine learning / data analytics algorithm, for both ε-differential privacy and (ε,λ)-differential privacy.
2	A rigorous study and understanding of the fundamental trade-off between privacy and utility (i.e. accuracy of the considered machine learning / data analytics algorithm) may be difficult because of algorithm's complexity.

PDA objectives in the SERUMS System	**Relevant KPIs and metrics**
Improve model privacy for given model utility	Associated with KPI 2.3 Enhanced Model Privacy that will be measured using the following metrics: (ε,λ)-differential privacy and utility.
Improve model utility for given privacy level	Associated with KPI 3.6 Data Analytics Model Utility And Model Privacy and KPI 4.1 Data Analytics Model

	Utility; that will be measured using the following metrics: (ε,λ)-differential privacy and utility.

2.3.6 Distributed Ledger Technology (DLT)

Distributed Ledger Technology is a new type of database system that allows multiple stakeholders to confidently and securely access to the same data and information in a controlled way. Transactions or data are stored in a ledger that is distributed among interested parties that are participating in an established network. The participating organisations in the blockchain network will be able access the data that they are entitled to without the need of a central party. All actions performed with regards to the changes of records in the blockchain will leave an immutable audit trail.

DLT Technical challenges	
1	Privacy: Have the right balance to address the traceability of the activities while maintaining the confidentiality.
2	Governance: Establish a new norm that are accepted by all stakeholders for shared ledgers. This is specially challenging when technology landscape and data structure varies significantly.
3	Scalability & Latency: Developing a solution that can handle the volume with expected latency. The performance of the individual machine could have impact over the performance of the network.

DLT objectives in the SERUMS System	**Relevant KPIs and metrics**
Segregate the permission to different part of the patient data; and embed the trust into the solution and empowers patients to decide about their own data (grand or restrict access). This will be achieved by providing a more granular access to the patient record.	This is associated with **“**KPI 2.4 Granular access to patient record”. This KPI will be measured by identifying the “Possibility to specify granular access rules over the patient record”
Increase the level of transparency and security with regards to handling of patient data. This will be achieved by enabling the creation of an immutable audit trail of all activities and actions from all the participating organisations in the blockchain network.	This is associated with “KPI 2.5 Authorization data integrity”. This KPI will be measuring how resilience the system is handling the authorisation data.

2.3.7 Verification of Technologies (VOT)

Verification of technologies is a set of approaches and tools used to validate that the proposed solutions will meet the formal requirements and their aims to secure health care services. For the validation, requirements must be expressed in a formal language, and by means of modelling, simulation and verification, the proposed solutions will be checked for meeting these requirements. Results of the checks can mathematically guarantee that the requirements are met. For the security aspect VOT involves modelling of various attacks on the system and proving that the system is sustainable against them.

VOT Technical challenges	
1	Build and maintain formal models of the proposed solutions that catch their specifics.
2	Employ formal methods for validation of the models.
3	Model various attacks on the system.

VOT objectives in the SERUMS System	**Relevant KPIs and metrics**
Check the requirement satisfaction	Not directly associated with any KPIs. Its role is supportive for the project.
Evaluate the access control	Associated with KPI 2.2 Data Breaches and 2.5 Authorization Data Integrity, measured by simulation.
Evaluate the vulnerability of the proposed solutions	Associated with KPI 1.3 System Vulnerability. This will be measured by modelling a number of attacks that system is meant to be resilient to.

3 SERUMS Expected Impacts and Associated Success Indicators

SERUMS aims to achieve significant impact in each area that has been identified in the SU-TDS-02-2018 call, providing significantly more secure smart health care provision, with significantly reduced potential for data breaches, and significantly improved patient trust and safety. This chapter provides a detailed description of the success indicators that will be used for measuring SERUMS progress and specific impact in terms of: **i)** Improved security of Health and Care services, data and infrastructures; **ii)** Less risk of data privacy breaches caused by cyber-attacks; and **iii)** Increased patient trust and safety. In particular, it provides clear definitions of the Key Performance Indicators (KPIs), along with their corresponding metrics, as well as the Baseline and the Trial measurements that will be used for measuring the success indicators. Moreover, information about the contribution of the various SERUMS tools/technologies and techniques in achieving the success indicators, as well as the definitions and measurements of the Key Performance Indicators (KPIs), is provided.

3.1 Expected Impact 1: Success Indicators and KPIs

The Success Indicator that will be used for measuring SERUMS progress and specific impact in terms of "Improved security of Health and Care services, data and infrastructures", is:

- **S1)** Quantifiable improvement in secure provision of health and care services (try to improve by a factor of 2), evidenced by reduced vulnerability of the Smart Health Centre to common cyber-attacks, as measured by standard indexes determining system resilience, robustness and availability during and after the attacks.

Below, the various SERUMS tools/technologies and techniques contributing to S1, clear definitions of the Key Performance Indicators (KPIs) along with their corresponding metrics, as well as the Baseline and the Trial measurements that will be used for measuring S1, are provided.

S1) Quantifiable improvement in secure provision of health and care services (try to improve by a factor of 2), evidenced by reduced vulnerability of the Smart Health Centre to common cyber-attacks, as measured by standard indexes determining system resilience, robustness and availability during and after the attacks.

SERUMS' Technologies Contributing in Achieving the Success Indicator

Personalized User Authentication (PUA):

- By providing personalized and "best-fit" password policies (in terms of password type such as textual *vs.* graphical; design types such as generic *vs.* familiar images), we aim to achieve a quantifiable improvement in both security (*e.g.*, users will avoid selecting predictable hotspots when they are familiar with an image), and memorability since users will be able to attach meaning to the content of the image.
- By achieving more memorable passwords, users will not need to follow coping strategies (*e.g.*, write down their passwords) affecting positively the password security.
- Through flexible, preference-based passwords, we aim to decrease capture attacks (*e.g.*, switch password type when user is in a public space to avoid shoulder surfing attacks).
- Through familiar images, users will select non-hotspots which will harden the guessability of selections on an image by a brute-force attack.

Smart Patient Record (SPR):

- By centralising each patient's data and storing it in a per-patient structure, the system will allow for each patient's record to be individually encrypted. This will prevent any large scale data leaks from being possible.

Verification of Technologies (VOT):

- The development of verification technologies to validate that the proposed solutions (*i.e.*, patient record privacy, standards and legal compliance, fabricated data quality, etc.) will meet the formal requirements and their aims to secure health care services.

Key Performance Indicators and SERUMS Technologies Associated

KPI 1.1: Guessability	**PUA**

Metrics:

This KPI will be measured using the following metrics:

- **Key space:** The set of all different permutations of a key. The key space range is determined by the adopted password policy which declares number of unique codes and password length.
- **Theoretical entropy:** The expected value (in bits) of the information contained in a string. The primary difference between key space and entropy is that key space is an absolute measure of maximum combinations, whereas entropy is related to how users select from the key space.
- **Practical entropy:** Metric that will be used to measure how random (strong) a text password is based on the user's actual selections. The more random, the more difficult it is to guess passwords.
- **Guess number:** Actual number of tries required to guess the password.
- **Textual password complexity:** A metric that describes how complex a textual password is based on the users' selection of characters.
- **Graphical password complexity:** A metric that describes how complex a graphical password is based on the users' image selections and gestures.
- **Push notification accuracy:** Measures the accuracy of the users' approvals of push notifications.

Trial Measurements:

Key space and Theoretical and Practical Entropy

We will calculate the theoretical key space, the theoretical entropy and the practical entropy of the generated authentication keys (textual and graphical). Key space (k_p) is defined as the range of different possible values of a key. Entropy is a measure on how difficult it is to guess a password [Burr et al., 2006]. In particular, entropy is measured as the expected value (in bits) of the information contained in a string [Shannon, 1949], and can be related to authentication key strength by providing a lower bound on the expected number of guesses to find a text [Massey, 1994]. The primary difference between key space and entropy is that key space is an absolute measure of maximum combinations, whereas entropy is related to how users select from the key space. The password key space (k_p) can be related directly to the maximum entropy as follows [O'Gorman, 2003]:

$$H_{max} = log_2k_p \text{ [bits]}$$

Furthermore, a true measure of Shannon's theoretical entropy cannot be computed in cases of user-chosen authentication keys since users tend to choose more memorable than random keys. Thus, in the analysis we will primarily consider practical entropy of the generated keys following a variation of Shannon's entropy calculation described and used in Komanduri et al. [2011] and Shay et al. [2010]. Since Shannon's formula allows to calculate in an additive manner, the adjusted calculation formula measures the practical entropy based on the various facets of the generated authentication keys by considering the placement of each character class (lower-case, upper-case, numbers, symbols) and image, and the content of each character and image. The final entropy is the summation of the entropy calculation of each facet.

Guess number

For textual passwords, we will assess the strength of user-generated password keys using Carnegie Mellon University's Password Guessability Service (PGS) [Ur et al., 2015]. PGS estimates plaintext passwords' "guessability"; how many guesses a particular password-cracking algorithm with particular training data would take to guess a password. For running the password guessability calculations, PGS uses four high-level approaches to password cracking: *i)* using the software tool oclHashcat; *ii)* using the software tool John the Ripper; *iii)* using probabilistic Markov models; and *iv)* using a probabilistic context-free grammar implementation (PCFG).

For graphical passwords, we will assess the strength of user-generated graphical password keys by measuring their resistance to an offline brute-force attack. We will implement a brute-force attack that will check all possible permutations of graphical keys, starting from the upper left corner of the image and traversing it row-by-row. We will measure guessability by calculating the average "guesses" performed per user until each corresponding graphical password is guessed correctly.

Textual password complexity

Textual password complexity will be calculated based on state-of-the-art password strength meters (*e.g.*, [[12][13][14]]).

Graphical password complexity

Graphical password complexity will be calculated, using the equation developed by Sun et al. as follows:

$$PS_P = S_p \, x \, log_2 \, (L_p + I_p + O_p)$$

In the above equation, S_p is the size of the password (*i.e.*, total number of images); L_p is the physical length of the password (*i.e.*, the sum of the Euclidean distances between the selected images of the password); I_p is the total number of intersections (*i.e.*, when two non-consecutive line segments have a common point); and O_p is the number of overlaps of the password pattern (*i.e.*, when a line segment of the password pattern is covered by another segment). The higher the score, the more complex the password is.

Push notification accuracy

Accuracy of the push notification method will be assessed through False Acceptance Rate (FAR), False Reject Rate (FRR), Failure To Enroll (FTE), Failure to Acquire (FTA).

Relation of the metrics with the Use-cases

The aforesaid metrics will be measured in the use cases of ZMC and FCRB. Relevant steps in the use cases are:

A. User needs to ***register*** *to the SERUMS system and* ***create*** *his/her password*

- Most of the metrics of this KPI are calculated beforehand based on the user authentication policy applied at each end-user organization, and the one applied in the SERUMS system. Hence, there is no specific use-case that facilitates the measurement of this metric.

Specifically, these metrics are: *key space*, *theoretical entropy*, *practical entropy* and *guess number* (based on state-of-the-art works and guidelines).

- Textual password complexity is calculated at run-time using client-side scripting when the user enters his/her textual password.
- Graphical password complexity is calculated at run-time using client-side scripting when the user enters his/her gestures on the image.

B. User needs to ***login*** *to the SERUMS system with the authentication option (s)he prefers*

- After successfully entering his/her password, a push notification is sent to the user's mobile device for approval. The mobile application that will be developed for this purpose (in D5.3) will facilitate the measurement of this metric.

Weighting Scheme of the metrics towards the KPI

The following weights have been defined by the expert partners of the project based on the importance and impact of the metric in the estimation of KPI value. A scale from 0 to 3 is used.

Metric	**Weight**
Key space	0
Theoretical entropy	1
Practical entropy	2
Guess number	3
Textual password complexity	2
Graphical password complexity	2
Push notification accuracy	2

Baseline Measurements:

Baseline measurements will be the same as the trial measurements (in cases where the authentication type is the same) and will be measured based on the currently applied user authentication types and policies of the end-users (control group). These will be compared with the trial measurements of the proposed PUA (experimental group).

Note: Several metrics cannot be applied in the baseline measurement, either because the end-user organization applies a different authentication type compared to the one suggested in SERUMS (*i.e.*, picture passwords, push notifications)[1], or due to security reasons, in which we cannot get the data relevant to the metric (*i.e.*, a database instance of hashed passwords to calculate practical entropy and guess number).

In summary, the following metrics cannot be calculated for the baseline evaluation:

- Practical entropy; instead we will consider state-of-the-art works and results (*e.g.*, [15]-[18]) which provide estimates of practical entropy of different password policies.

[1] *A report on current authentication policies and practices of each organization is reported in Deliverable 5.1 - Initial Report on Security Metrics and Authentication Policies*

- Guess number; instead we will consider state-of-the-art works and results (*e.g.*, [15]-[18]) which provide estimates of guess numbers of different password policies.
- Graphical password complexity
- Push notification accuracy

How Impact on the Success Indicator will be measured

The Baseline Measurements **(Key Space, Theoretical Entropy, Practical Entropy, Guess Number, Textual Password Complexity)** will be compared with the Trial Measurements. An increase in the Trial Measurement values implies a quantifiable (%) improvement in secure provision of health and care services.

KPI 1.2: Password Leaks (through Social Engineering)	**PUA**

Metrics:

This KPI will be measured using the following metrics:

- **Memory time:** The greatest length of time between a password creation and the last successful password login using the same password will be measured. Large memory times indicate higher memorability. Memorable passwords lead to potentially less social engineering-based password leaks because users will not need to follow coping strategies (e.g., write down their passwords).
- **Shoulder surfing success rate:** Measured through direct observations with real users trying to steal the password of a victim by looking on the victim's screen**.**

Trial Measurements:

Memory time

Following existing approaches for measuring the memorability of a password [Stobert et al., 2013], memory time will be measured over time by considering the login attempts of the end-users. As an additional measure of memorability, the number of password resets per participant will be used. The longer the memory time, the higher the memorability, while the less the number of password resets per participant, the higher the memorability.

Shoulder surfing success rate

Following state-of-the-art approaches for measuring shoulder surfing attacks (*e.g.*, von Zezschwitz et al., 2015), shoulder surfing will be measured with participants that will act as shoulder surfers which will perform a hypothetical shoulder surfing attack. Shoulder surfing attacks will be based on a one-time view of the input followed by three guesses. For each password-entry, we will compute the binary success (true/false) and the relative success rate (overlap of correct digits) based on the best of the three guesses.

Relation of the metrics with the Use-cases

The aforesaid metrics will be measured in the use cases of ZMC and FCRB.

Relevant Step in Use-case: User needs to ***login*** *to the SERUMS system with the authentication option (s)he prefers*

- Memory time will be calculated based on the actual login attempts and number password resets in the system.
- Shoulder surfing will be measured through a controlled lab study with participants that will act as shoulder surfers which will perform a hypothetical shoulder surfing attack.

Weighting Scheme of the metrics towards the KPI

The following weights have been defined by the expert partners of the project based on the importance and impact of the metric in the estimation of KPI value. A scale from 0 to 3 is used.

Metric	Weight
Memory time	3
Shoulder surfing	1

Baseline Measurements:

Baseline measurements will be the same as the trial measurements and will be measured based on the currently applied user authentication types and policies of the end-users (control group). These will be compared with the trial measurements of the proposed PUA (experimental group).

How Impact on the Success Indicator will be measured

The Baseline **Memory time** and **Shoulder surfing success rate** Measurements will be compared with the Trial Measurements. An increase in the Trial Measurement **Memory time** and decrease of **Shoulder surfing success rate** values, implies a quantifiable (%) improvement in secure provision of health and care services.

KPI 1.3: System Vulnerability	**SPR & VOT**

Metrics:

This KPI will be measured using the following metrics:

- **System Maintenance:** The measure of how up-to-date the system is, considering the operating system version, patch updates, antiviruses etc. assessed by a questionnaire. This will allow us to see how vulnerable the system is to the known attacks.
- **System Security:** The measure of how susceptible the system is via penetration testing as well as the security of the authentication methods. The types of penetration that we will use will be both external network and internal network penetration testing. This will allow us to see how vulnerable the system is from the outside as well as once they have gained some form of access.

Trial Measurements:

- **System Maintenance:** The measure of how up-to-date the system is, considering the operating system version, patch updates, antiviruses etc. assessed by a questionnaire. This will allow us to see how vulnerable the system is to the known attacks.
- **System Security:** The measure of how susceptible the system is via penetration testing as well as the security of the authentication methods. The types of penetration that we will use will be both external network and internal network penetration testing. This will allow us to see how vulnerable the system is from the outside as well as once they have gained some form of access.

Relation of the metrics with the Use-cases

The aforesaid metric will be measured in all the use cases defined in D7.3.

Weighting Scheme of the metrics towards the KPI

The following weights have been defined by the expert partners of the project based on the importance and impact of the metric in the estimation of KPI value. A scale from 0 to 3 is used.

Metric	Weight
System maintenance	1
System security	3

Baseline Measurements:

System maintenance:

The baseline measurement will be the same as the trial measurements and will be measured with the same questionnaire.

System security

As a baseline we consider 0 attacks the system is secure against.

How Impact on the Success Indicator will be measured

There is an assumption that the system will continue to be patched, and the firewall/antivirus software will be kept up to date. As such, the measurement of the improved system security will be based on the understanding of the additional layers of security that our system introduces, including the individual encryption of each patient's data and the use of blockchain to control the access to the system.

Weighting scheme of the KPIs towards the Success Indicator 1

The following weights have been defined by the expert partners of the project based on the importance and impact of the KPI in the estimation of success indicator value. A scale from 0 to 3 is used.

KPI	Weight
KPI 1.1: Guessability	1
KPI 1.2: Password leaks (through social engineering)	2
KPI 1.3: System vulnerability	2*

** While system vulnerability is a vital part of the project, the current laws surrounding data protection and the minimum security associated with storing sensitive data is already very high. As such we are unlikely to be able to improve this greatly.*

3.2 Expected Impact 2: Success Indicators and KPIs

The Success Indicator that will be used for measuring SERUMS progress and specific impact in terms of "Less risk of data privacy breaches caused by cyber-attacks", is:

- **S2)** Significantly reduced risk of data privacy breaches (try to achieve a 75% reduction), evidenced by quantitative metrics showing the quantity of private data that is revealed through a number of common cyber-attacks.

Below, the various SERUMS tools/technologies and techniques contributing to S2, clear definitions of the Key Performance Indicators (KPIs) along with their corresponding metrics, as well as the Baseline and the Trial measurements that will be used for measuring S2, are provided.

S2) Significantly reduced risk of data privacy breaches (try to achieve a 75% reduction), evidenced by quantitative metrics showing the quantity of private data that is revealed through a number of common cyber-attacks.	
SERUMS' Technologies Contributing in Achieving the Success Indicator	

Credential Hardening (CH):
• Through novel credential hardening mechanisms we aim to secure credentials stored at the server-side and detect password guessing attempts.
Smart Patient Record (SPR):
• By centralising each patient's data and storing it in a per-patient structure, the system will allow for each patient's record to be individually encrypted. This will prevent any large scale data leaks from being possible.
Privacy-preserving Data Analytics (PDA):
• By developing new and enhancing current approaches in privacy preserving machine learning we will increase the level of privacy preserved by current approaches while keeping a similar level of utility.
Verification of Technologies (VOT):
• The development of validation technologies that include quantification of how well the proposed solutions reduce the risk of privacy breaches.
Distributed Ledger Technology (DLT):
• By using distributed ledger technology, the data is kept encrypted and stored distributed over the nodes on the network thus no central point of failure. Hacker needs to take down the collective power of the network to compromise any data. In case a node is corrupted, the network can restore the data based on any uncorrupted node.	

Key Performance Indicators and SERUMS Technologies Associated	
KPI 2.1: Password Cracking Resistance	**CH**
Metrics: This KPI will be measured using the following metrics:	

- **Password cracking rate:** It will be measured in a leaked database storing hardened credentials through an offline brute-force attack.

Trial Measurements:

Password cracking rate

The rate of the passwords successfully cracked will be measured through an offline brute-force attack performed in the leaked database that stored the hardened credentials.

Relation of the metrics with the Use-cases

The aforesaid metrics will be measured in the use cases of ZMC and FCRB.

Relevant Step in Use-case is: User needs to ***register*** *to the SERUMS system and* ***create*** *his/her password*

Password cracking rate will be measured after all users create their passwords that will be stored in a hashed format in the database. An offline brute-force attack will be run in the database that stored the credentials.

Note: Due to the sensitive nature of running a brute-force attack on hashed user passwords, we will run the attack on synthetic user passwords that will be generated based on the current organization's (baseline) vs. proposed credential storage approach and policies.

Weighting Scheme of the metrics towards the KPI

N/A. There is only one metric that is measured.

Baseline Measurements:

Baseline measurements will be the same as the trial measurements and will be measured based on the credential storing approaches currently used by the end-users (control group). These will be compared with the trial measurements of the proposed CH (experimental group).

How Impact on the Success Indicator will be measured

Standard password-cracking rate with de facto tools will be compared when credentials are stored using typical cryptographic hash functions and when CH is in place.

KPI 2.2: Data Breaches	**SPR & VOT**

Metrics:

This KPI will be measured using the following metrics:

- **Data Breaches:** The measure of data that will be able to be accessed by unauthorised or inappropriate sources. Through a verification we will take measurements on how much data can be accessed by both, an unknown user and a known user, for unauthorised reasons.

Trial Measurements:

Data Breaches

This will cover how much patient data can be accessed at any one time by staff members from different departments i.e., reception, nurse, doctor. Additionally it will record the level of access available from different stations. This will include whether removable media can allow for the copying of data, as well as whether all data for all patients can be accessed. These will be measured by verification.

Relation of the metrics with the Use-cases

The aforesaid metric will be measured in all the use cases defined in D7.3.

Weighting Scheme of the metrics towards the KPI

N/A. There is only one metric that is measured.

Baseline Measurements:

The baseline measurement will be will be measured with a graded questionnaire. This will capture the risk associated with unauthorised access.

How Impact on the Success Indicator will be measured

The volume and nature of the data that can be accessed during the trial period will be compared. A reduction in either the unauthorised data accesses or data accessed for inappropriate reasons implies an improvement in data breaches. The comparison will be made between the questionnaires from both the baseline and trial measurements.

KPI 2.3: Enhanced Model Privacy	**PDA**

Metrics:

This KPI will be measured using the following metrics:

- (e; δ)-Differential Privacy: We use the mathematical framework of (e; δ)-differential privacy to measure how well the privacy of the used training data set is preserved in the output of the trained model.
- Model Utility: The model utility will be measured as the difference between the model's prediction and the expected result in the validation data set.

Trial Measurements:

The two properties, privacy and utility, that we measure using the defined metrics, are competing properties. Enhancing privacy always leads to reduced utility. Therefore, the measurement of this KPI is strongly associated to KPI 3.6 (Data Analytics Model Utility and Model Privacy) and KPI 4.1 (Data Analytics Model Utility).

In the trial measurements we use benchmark datasets to train models using state-of-the-art privacy preserving algorithms and train models using our novel approach. To measure the enhancement of model privacy we compare the achieved level of privacy of the models for the same model utility.

Relation of the metrics with the Use-cases

The metrics will be used in the USTAN use case mentioned in D7.3 in prediction of the toxicity level in chemotherapy treatment.

Weighting Scheme of the metrics towards the KPI

The following weights have been defined by the expert partners of the project based on the importance and impact of the metric in the estimation of the KPI value. A scale from 0 to 3 is used.

Metric	**Weight**
(e; δ)-differential privacy	3
Model Utility	3

Baseline Measurements:

The baseline measurement will be the same as the trial measurements.

How Impact on the Success Indicator will be measured

Enhancing the level of privacy while keeping the model utility on the same needed level will lead to a reduced risk of privacy breaches without losing accuracy. The impact on the Success Indicator will be measured as the factor of privacy enhancement.

KPI 2.4: Granular access to patient record	**DLT**

Metrics:

This KPI will be measured by the Possibility to specify granular access rules over the patient record.

Trial Measurements:

The DLT solution allows to specify granular data access rules. During the trial measurement, we will assess the number of levels a patient record can be broken down into separate data groups. For each one of these data groups, an access rule can be created.

Relation of the metrics with the Use-cases

- Use case ZMC: Patients have the possibility to view existing rules, create additional rules to permit or restrict access for a selected set of data.
- Use case FCRB: When health professionals need to access the new measurement data, it will be checked whether the requestor has the corresponding permission to access this patient’s data. When positive, a request will be triggered to retrieve the data. Permission rules to grant or restrict access can be defined by the patient for health organizations, individuals or groups. Although default rules for the caregiver to access the patient is defined by the hospital administrator according to national regulations. Patients have the possibility to create specific rules to permit or restrict access.

Weighting Scheme of the metrics towards the KPI

N/A. There is only one metric that is measured.

Baseline Measurements:

Today in the consortium, there is no equivalent solution in place to manage multiparty access of the patient data. (Level 1).

How Impact on the Success Indicator will be measured

We have defined 4 levels of permission granularity of patient record access. With 1-4 where level 4 is the most satisfactory level. The DLT solution aim to reach level 4.

1. No digital access management of the patient record
2. Access can be managed by the organisations (e.g. hospital) at patient record level
3. Access can be managed by the organisations (e.g. hospital) at granular level (e.g. subset of the patient record)
4. Access can also be managed by the patient

KPI 2.5: Authorisation Data Integrity	**DLT & VOT**

Metrics:

In case a party on the DLT network is being compromised and it has been identified that data has been tempered with, the solution is able to identify the exact data that has been tempered with and retrieve the original value

This KPI will be measured using the following metrics:

- The amount of compromised data that can be identified and recovered

Trial Measurements:

In the Trial measurement, a simulated event can be organised with the purpose to temper part of the authorisation related data. After the event, we will access the total % of data that can be identified and the % of the data items that can be recovered.

Relation of the metrics with the Use-cases

- This metric is not related to interactions directly with patient thus no direct link with the use cases.

Weighting Scheme of the metrics towards the KPI

N/A. There is only one metric that is measured.

Baseline Measurements:

Today, in the SERUMS consortium, there is no equivalent solution in place to discover what authorisation data has been compromised when access log is also deleted.

How Impact on the Success Indicator will be measured

The solution provides new possibility whereas today it is not possible to achieve this.

Weighting scheme of the KPIs towards the Success Indicator 2

The following weights have been defined by the expert partners of the project based on the importance and impact of the KPI in the estimation of success indicator value. A scale from 0 to 3 is used.

KPI	Weight
KPI 2.1: Password Cracking Resistance	3
KPI 2.2: Data Breaches	3*
KPI 2.3: Enhanced Model Privacy	1
KPI 2.4: Granular access to patient record	2
KPI 2.5: Authorisation Data Integrity	1

** The ability for the patient to control access to their data is one of the core components of the SERUMS project*

3.3 Expected Impact 3: Success Indicators and KPIs

The Success Indicators that will be used for measuring SERUMS progress and specific impact in terms of “Increased patient trust and safety” are:

- **S3)** Quantifiable improvement in levels of patient trust in the provision of smart health care (try to improve by a factor of 2), evidenced by patient surveys and questionnaires.
- **S4)** Quantifiable improvement in patient safety (try to improve by a factor of 2), evidenced by reduced risk of harm through incorrect treatments or medicines mediated by reduced risk of tampering with medical records, and measured vulnerabilities of connected medical systems.

Below, the various SERUMS tools/technologies and techniques contributing to S3 and S4, clear definitions of the Key Performance Indicators (KPIs) along with their corresponding metrics, as well as the Baseline and the Trial measurements that will be used for measuring S3 and S4, are provided.

S3) Quantifiable improvement in levels of patient trust in the provision of smart health care (try to improve by a factor of 2), evidenced by patient surveys and questionnaires
SERUMS’ Technologies Contributing in Achieving the Success Indicator

Personalized User Authentication (PUA):
• Through personalized passwords we aim to improve perceived password usability, memorability, security, user acceptance and trust.
Smart Patient Record (SPR):
• By allowing patients to control who has access to their data and what it is being used for we will see an increase in the trust patients have in smart health care.

Privacy-preserving Data Analytics (PDA):

- With the development of distributed privacy-preserving deep learning models including transfer-learning and multitask approaches, models can be trained using more than a single data source without the need of actually sharing private data, which leads to a higher level of utility of trained models. Developing new methods will enable higher levels of model utility while keeping similar levels of privacy.

Key Performance Indicators and SERUMS Technologies Associated

KPI 3.1: Perceived Usability	**PUA**

Metrics:

This KPI will be measured using the following metrics:

- **Questionnaires:** Usability and User Experience questionnaires will be designed for the assessment of perceived usability. Specific rules will be used for producing scores based on the answers of respondents.
- **Interviews:** Qualitative interviews will be conducted, which will enable the interviewer to collect detailed information from the interviewees regarding the perceived usability.
- **Focus Groups:** Focus groups will be conducted to elicit end-users' perceptions about the perceived usability.

Trial Measurements:

Questionnaires (usability, UX, etc.)

Scores of the perceived usability of PUA will be calculated based on the answers of respondents. For this purpose, usability and user experience questionnaires will be designed for the assessment of perceived usability. Accredited questionnaires such as SUS, AttrakDiff, etc. will also be used for measuring perceived usability.

Interviews

Thematic content analysis will be used in order to find common patterns across the data set on the perceived usability of PUA.

Focus Groups

The qualitative analysis of Focus Groups results will be a five-step process that includes Data Grouping, Information Labels, Knowledge (Findings), Theory, and Implications.

Relation of the metrics with the Use-cases

The aforesaid metrics will be measured in the use cases of ZMC and FCRB. Relevant steps in the use cases are:

*A. User needs to **register** to the SERUMS system and **create** his/her password*

*B. User needs to **login** to the SERUMS system with the authentication option (s)he prefers*

After completing the interaction with the user authentication system (at the end of the use-case), the users respond to a series of questions that relate to their perceived usability with regards to the password creation task and the login task

Weighting Scheme of the metrics towards the KPI

Not applicable with this KPI.

Baseline Measurements:

Baseline measurements will be the same as the trial measurements and will be measured based on the currently applied user authentication types and policies of the end-users (control group). These will be compared with the trial measurements of the proposed PUA (experimental group).

How Impact on the Success Indicator will be measured

The Baseline Measurement will be compared with the Trial Measurement. Statistical tests will be run, where applicable, to determine whether there are significant differences in the perceived usability between the currently applied user authentication types and policies of the end-users (control group) and the proposed PUA (experimental group).

KPI 3.2: Perceived Memorability	**PUA**

Metrics:

This KPI will be measured using the following metrics:

- **Questionnaires:** Specific questionnaires will be designed for the assessment of perceived memorability. Specific rules will be used for producing scores based on the answers of respondents.
- **Interviews:** Qualitative interviews will be conducted, which will enable the interviewer to collect detailed information from the interviewees regarding the perceived memorability.
- **Focus Groups:** Focus groups will be conducted to elicit end-users' perceptions about the perceived memorability.

Trial Measurements:

Questionnaires (usability, UX, etc.)

Scores of the perceived memorability of PUA will be calculated based on the answers of respondents.

Interviews

Thematic content analysis will be used in order to find common patterns across the data set on the perceived memorability of PUA.

Focus Groups

The qualitative analysis of Focus Groups results will be a five-step process that includes Data Grouping, Information Labels, Knowledge (Findings), Theory, and Implications.

Relation of the metrics with the Use-cases

The aforesaid metrics will be measured in the use cases of ZMC and FCRB.

Relevant Step in Use-case: User needs to ***login*** *to the SERUMS system with the authentication option (s)he prefers*

After completing the interaction with the login task, the users respond to a series of questions that relate to their perceived memorability with regards to the login task

Weighting Scheme of the metrics towards the KPI

Not applicable with this KPI.

Baseline Measurements:

Baseline measurements will be the same as the trial measurements and will be measured based on the currently applied user authentication types and policies of the end-users (control group). These will be compared with the trial measurements of the proposed PUA (experimental group).

How Impact on the Success Indicator will be measured

The Baseline Measurement will be compared with the Trial Measurement. Statistical tests will be run, where applicable, to determine whether there are significant differences in the perceived memorability between the currently applied user authentication types and policies of the end-users (control group) and the proposed PUA (experimental group).

KPI 3.3: Perceived Security	PUA

Metrics:

This KPI will be measured using the following metrics:

- **Questionnaires:** Specific questionnaires will be designed for the assessment of perceived security. Specific rules will be used for producing scores based on the answers of respondents.
- **Interviews:** Qualitative interviews will be conducted, which will enable the interviewer to collect detailed information from the interviewees regarding the perceived security.
- **Focus Groups:** Focus groups will be conducted to elicit end-users' perceptions about the perceived security.

Trial Measurements:

Questionnaires (usability, UX, etc.)

Scores of the perceived security of PUA will be calculated based on the answers of respondents.

Interviews

Thematic content analysis will be used in order to find common patterns across the data set on the perceived security of PUA.

Focus Groups

The qualitative analysis of Focus Groups results will be a five-step process that includes Data Grouping, Information Labels, Knowledge (Findings), Theory, and Implications.

Relation of the metrics with the Use-cases

The aforesaid metrics will be measured in the use cases of ZMC and FCRB. Relevant steps in the use cases are:

A. User needs to ***register*** *to the SERUMS system and* ***create*** *his/her password*

B. User needs to ***login*** *to the SERUMS system with the authentication option (s)he prefers*

After completing the interaction with the user authentication system (at the end of the use-case), the users respond to a series of questions that relate to their perceived security with regards to the user authentication system

Weighting Scheme of the metrics towards the KPI

Not applicable with this KPI.

Baseline Measurements:

Baseline measurements will be the same as the trial measurements and will be measured based on the currently applied user authentication types and policies of the end-users (control group). These will be compared with the trial measurements of the proposed PUA (experimental group).

How Impact on the Success Indicator will be measured

The Baseline Measurement will be compared with the Trial Measurement. Statistical tests will be run, where applicable, to determine whether there are significant differences in the perceived security between the currently applied user authentication types and policies of the end-users (control group) and the proposed PUA (experimental group).

KPI 3.4: Trust in the proposed PUA scheme	**PUA**

Metrics:

This KPI will be measured using the following metrics:

- **Technology Acceptance Model:** Technology Acceptance Model questionnaires will be designed for the assessment of trust in the proposed PUA. Specific rules will be used for producing scores based on the answers of respondents.

Trial Measurements:

Technology Acceptance Model Questionnaire

Scores of the trust in the proposed PUA will be calculated based on the answers of respondents.

Relation of the metrics with the Use-cases

The aforesaid metrics will be measured in the use cases of ZMC and FCRB. Relevant steps in the use cases are:

*A. User needs to **register** to the SERUMS system and **create** his/her password*

*B. User needs to **login** to the SERUMS system with the authentication option (s)he prefers*

After completing the interaction with the user authentication system (at the end of the use-case), the users respond to a series of questions that relate to their perceived trust towards the user authentication system

Weighting Scheme of the metrics towards the KPI

Not applicable with this KPI.

Baseline Measurements:

Baseline measurements will be the same as the trial measurements and will be measured based on the currently applied user authentication types and policies of the end-users (control group). These will be compared with the trial measurements of the proposed PUA (experimental group).

How Impact on the Success Indicator will be measured

The Baseline Measurement will be compared with the Trial Measurement. Statistical tests will be run, where applicable, to determine whether there are significant differences in the trust between the currently applied user authentication types and policies of the end-users (control group) and the proposed PUA (experimental group).

KPI 3.5: Patient Trust	**SPR**

Metrics:

This KPI will be measured using the following metrics:

- **Questionnaires (perceived trust):** These will be a simple scaled questionnaire designed to record the level of trust in the hospital’s data management that the patients have. This questionnaire will be designed by our UX team in order to ensure that the questions are not leading.

Trial Measurements:

Questionnaires (perceived trust)

These will be used to gather quantitative values both before and after the process to measure how patients feel about their levels of trust.

Relation of the metrics with the Use-cases

The aforesaid metrics will be measured in all the use cases defined in D7.3.

Weighting Scheme of the metrics towards the KPI

N/A. There is only one metric that is measured.

Baseline Measurements:

An initial questionnaire will be given to patients to understand how they feel about the current state of their data’s management.

How Impact on the Success Indicator will be measured

The same questionnaire will be given to participants following a conversation in which the changes that have been implemented are explained. An increase in the score implies an improvement in perceived trust.

KPI 3.6: Data Analytics Model Utility And Model Privacy	**PDA**

Metrics:

This KPI will be measured using the following metrics:

- (e; δ)-Differential Privacy: We use the mathematical framework of (e; δ)-differential privacy to measure how well the privacy of the used training data set is preserved in the output of the trained model.
- Model Utility: The model utility will be measured as the difference between the model’s prediction and the expected result in the validation data set.

Trial Measurements:

The two properties, privacy and utility, that we measure using the defined metrics are competing properties. Enhancing privacy always leads to reduced utility. Therefore, the measurement of this KPI is strongly associated to KPI 2.3 (Enhanced Model Privacy) and KPI 4.1 (Data Analytics Model Utility).

In the trial measurements we use benchmark datasets to train models using state-of-the-art privacy preserving algorithms and train models using our novel approach. To measure the enhancement of model utility we compare the achieved model utility for the same level of model privacy. To measure the enhancement of model privacy we compare the achieved model privacy for the same level of model utility.

Relation of the metrics with the Use-cases

The metrics will be used in the USTAN use case mentioned in D7.3 in prediction of the toxicity level in chemotherapy treatment.

Weighting Scheme of the metrics towards the KPI

The following weights have been defined by the expert partners of the project based on the importance and impact of the metric in the estimation of the KPI value. A scale from 0 to 3 is used.

Metric	Weight
(e; δ)-differential privacy	3
Model Utility	3

Baseline Measurements:

Baseline measurements will be the same as the trial measurements.

How Impact on the Success Indicator will be measured

Enhancing the model utility while keeping the level of privacy on the same needed level will lead to better predictions which increases patient trust in provision of smart health care. Enhancing the model privacy while keeping the level of utility on the same level will lead increased patient trust that their data is not revealed. The impact will be measured as the difference between baseline and trial measurements.

Weighting scheme of the KPIs towards the Success Indicator 3

The following weights have been defined by the expert partners of the project based on the importance and impact of the KPI in the estimation of success indicator value. A scale from 0 to 3 is used.

KPI	**Weight**
KPI 3.1: Perceived usability	2
KPI 3.2: Perceived memorability	1
KPI 3.3: Perceived security	2
KPI 3.4: Trust in the proposed PUA scheme	3
KPI 3.5: Patient Trust	1*
KPI 3.6: Data Analytics Model Utility	1

** Due to the lifelong use of the health services, patients already have an inbuilt trust in the existing system. As such we are unlikely to bring an improvement, however it is important that we capture the results*

S4) Quantifiable improvement in patient safety (at least a factor of 2), evidenced by reduced risk of harm through incorrect treatments or medicines mediated by reduced risk of tampering with medical records, and measured vulnerabilities of connected medical systems.

SERUMS' Technologies Contributing in Achieving the Success Indicator

Privacy-preserving Data Analytics (PDA):

- With the development of distributed privacy-preserving deep learning models including transfer-learning and multitask approaches, models can be trained using more than a single data source without the need of actually sharing private data, which leads to a higher level of utility of trained models.

Key Performance Indicators and SERUMS Technologies Associated

KPI 4.1: Data Analytics Model Utility	**PDA**

Metrics:

This KPI will be measured using the following metrics:

- (e; δ)-Differential Privacy: We use the mathematical framework of (e; δ)-differential privacy to measure how well the privacy of the used training data set is preserved in the output of the trained model.
- Model Utility: The model utility will be measured as the difference between the model's prediction and the expected result in the validation data set.

Trial Measurements:

The two properties, privacy and utility, that we measure using the defined metrics are competing properties. Enhancing privacy always leads to reduced utility. Therefore, the measurement of this KPI is strongly associated to KPI 2.3 (Enhanced Model Privacy) and KPI 3.6 (Data Analytics Model Utility).

In the trial measurements we use benchmark datasets to train models using state-of-the-art privacy preserving algorithms and train models using our novel approach. To measure the enhancement of model utility we compare the achieved model utility for the same level of model privacy.

Relation of the metrics with the Use-cases

The metrics will be used in the USTAN use case mentioned in D7.3 in prediction of the toxicity level in chemotherapy treatment.

Weighting Scheme of the metrics towards the KPI

The following weights have been defined by the expert partners of the project based on the importance and impact of the metric in the estimation of the KPI value. A scale from 0 to 3 is used.

Metric	**Weight**
(e; δ)-differential privacy	3
Model Utility	3

Baseline Measurements:

Baseline measurements will be the same as the trial measurements.

How Impact on the Success Indicator will be measured

Enhancing the model utility while keeping the level of privacy on the same needed level will lead to better predictions which increases patient safety in provision of smart health care. The impact will be measured as the difference between baseline and trial measurements.

3.4 Formula for KPIs and Success Indicators Estimation: The AMPI method

As can be seen in Deliverable 7.3 the KPI consist of metrics, each of one of them having different units and ranges. This resulted in the problem of having to merge these numbers, sometimes being as diverse as 20 bits and 1.38E-23, into one single number (the KPI). For obvious reasons this was impossible to do by a simple arithmetic addition. The chosen method to achieve the calculations of the KPI has been the AMPI Index formula [19] that is shown below.

$$r_{ij} = \left[\frac{\left(y_{ij} - min\, y_i \right)}{\left(max\, y_i - min\, y_i \right)} \right]$$

As can be seen, to use this formula two limits have to be carefully chosen, since these will set the maximum and minimum range of the improvement and will not change from this initial report to the Final Evaluation of the SERUMS project.

Each of the intervals chosen for the measurements and KPIs (since some measurements are KPI by themselves) can be found in D7.3. The weights for every metric towards the KPI are set at the end of the section for every KPI.

4 Ethical Challenges

This chapter describes the ethical challenges that should be addressed in the SERUMS project.

4.1 Ethics: General Aspects on General Issues

To ensure a full understanding of the legal implications of involving the collection and processing of medical data as well as personally identifiable data in the project, all consortium partners will ensure that relevant legal provisions on the processing of data will be respected during the entire course of the project in accordance with key legislation. Relevant legislation includes:

- The Charter of Fundamental Rights of the EU;
- The Directive 95/46/EC;
- The Regulation Directive 2002/58/EC;
- The Directive 2006/24/EC of the European Parliament and of the Council for data protection inside the EU, that aims to protect individuals with regard to the processing of personal data and the free movement of such data;
- The Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data;
- SERUMS will also respect the Helsinki Declaration in its latest version;
- SERUMS will consider the opinions of the European Group on Ethics in Science and New technologies (as from 1998) and the European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data signed in Strasbourg on 28 January 1981.

The consortium is fully aware of the potential ethical pitfalls rising during the course of its research. To overcome potential ethical concerns, the consortium aims to adopt a common understanding of the ethical principles underlying the work performed in the project. All SERUMS work will strictly comply with the Directives listed above. Safety and Security will be dealt with by applying the relevant standards and directives (among others MDD, FDA, CE, EMC, ISO (ISO27001:2013/27002:2013), NEN (NEN7510:2017, 7512 en 7513), MedMij standards (NL) and detailed risk analysis.

The SERUMS clinical partners, “Clınic Foundation for Biomedical Research” (FCRB), “Zuyderland” (ZMC) and the University of St Andrews will apply for ethical approval from their respective ethical committees for conducting surveys and for interviews for requirements gathering, as well as for performing pilot studies of the developed technology in end-user settings. Data from monitoring equipment will be stored and analysed by the clinical partners FCRB and ZMC. For clarifying, health data from end-users of FCRB will be collected, transmitted, stored, and analysed at FCRB. Health data from end-users at ZMC will be stored at ZMC and analysed at ZMC. Survey and interview data will also be collected at FCRB or ZMC, respectively, and stored there. This anonymised data will be transmitted to other related research partners for analysis. Synthetic/fabricated data will be used for testing purposes. Particular care will be taken when transferring (anonymised) data across international boundaries. Therefore, the project objectives raise important ethical and legal issues and special attention will be given to the following points, directly related to the research performed by SERUMS:

- Patients prior, free, express and smart informed consent;
- Procedures of withdrawal in case a patient wishes to quit at any time;
- Design and implementation of legally compliant anonymization and pseudo-anonymization tools for patients data;
- A feedback procedure to the patient where necessary and agreed on in the informed consent. In case a problem arises with new legislation relating to health/genetic data collection, data access or patients rights, the management of the project will evaluate the situation and take

appropriate actions. The legal responsibility will always remain within the consortium, and according to recommendation n 83 of the European Council;

- The use of several data for SERUMS is applicable inside the European legal framework, mainly on privacy and data protection and also local governance data protection laws (LOPD) and according to recommendation n 83 of the European Council;
- The study protocol will be submitted to the local Institutional Ethics Committees in accordance with the laws concerning observational studies. All documentation and legal clearances for patient information and data management will have to be approved before the beginning of recruitment in conformity with local regulations;
- The participation of a patient in the SERUMS proposal is always voluntary. Extraordinary care will be taken to receive appropriate and legally valid informed consent to the collection of, access to, joining of and analysing the patients health data. In particular, such research will only be carried out with the prior, free, and expressed informed consent of the person concerned, in accordance with all applicable international laws and ethical guidelines related to the protection of personal data as well as internationally accepted rules on bioethics and human rights. Patients, having given their consent to the processing of their data, shall be able to withdraw such consent at any time and for any reason without any disadvantage or penalty on the same basis as proposed by other large-scale research undertakings. Participation, non-participation or withdrawal from the SERUMS proposal has no impact on the clinical care they receive. Informed consent will follow the procedures established by the WMA Declaration of Helsinki.

As described above, the FCRB and ZMC medical use case data will be the main legal and ethical concern of the project. In order to maintain an adequate ethical methodology, the consortium will ensure that data is only processed when necessary for the purposes of the project, and when the benefits expected from the outcome of the research outweigh the any potential negative impacts or risks on the individuals, and that anonymization is used, to reduce risks of data loss or leakage. In order to ensure that all research is carried out in accordance with the relevant guidelines and legislations, SERUMS will include an Ethical Advisory Board constituting the following persons for the whole lifetime of the project:

- Dr. Juliana Bowles (USTAN),
- Dr Michael Vinov (IBM),
- Mr. Andreas Vermeulen (SOPRA) and
- Mr. Mark Mestrum (ZMC) and
- Mr. Santiago Iriso (FCRB),

This board will maintain oversight of all personal/sensitive/confidential data, restrict access to that data, enforce the use of masking etc., techniques where needed to protect data, and be responsible for ensuring overall compliance with all relevant legislation, requirements and ethical standards.

The application of the legal framework is twofold. On the one hand, the functioning of the envisaged end-product must be legally compliant and privacy enhancing, from within the services design. This means that the choices of the consortium will be inspired by privacy and data protection requirements from the early stages in the project and the project solution will not only visually embrace privacy in its system design but also throughout the development. On the other hand, legal compliance is also required for the formal development of the project solution. This means that also on the road to the end-product privacy principles will shape the decisions of the consortium. In all stages of the project the privacy of the end-users will be considered to meet the principles of the proposed data protection legal framework.

4.2 Data Management and Ethical Issues

Privacy of genetic, biological, and clinical data will be guaranteed. No personally identifiable information will be retained by the consortium team during or after the SERUMS project. Each patient participating in the study will be identified by a code number, and only the code will be used for data collection and analysis. Data transfer among institutions and to project partners involved in the study project will be protected by local security systems, mechanisms, and best practice. Data collected will not be sold, disclosed to third parties, nor held or encoded in an insecure manner, nor will any collection of data about criminal records, financial information, or data considered by community standards to be of a personal nature. Data will only be used during the course of the project, will be used only for the limited and declared purposes of the project as disclosed, and in accordance with all national law and with best practice guidelines for ethical research as recommended by EU ethical policy documents. The project Ethics Committee will convene regularly, and constantly monitor the project for any potential ethics issues.

4.3 Legal Framework

The project has been developed according to the indications contained in The Charter of Fundamental Rights of the European Union and The Declaration of Helsinki (Recommendation For Conduct Of Clinical Research, the Convention of the Council of Europe on Human Rights and Biomedicine- Oviedo 1997, and the Additional Protocol on the Prohibition of Cloning Human Beings – Paris 1998), according to:

- Art. 1: respect of the dignity of the human being as a whole;
- Art. 2: granting that the collected information will be used only in service of the human being and his right to life;
- Art. 3: II 1-III 2, 3c dealing with medicine and biology, assure the application of the rule of informed consent to collect and store data; transparency of the scope and employment of the collected medical data (ref. also to Art. 8); preventing and prohibiting the misuse of the stored information for eugenic purposes; preventing and prohibiting commerce of the human body for personal gain; preventing and prohibiting cloning;
- Art. 7: respect of the right to private life of the individual;
- Art. 21: preventing and avoiding any kind of discrimination based on the collected information;
- Art. 23: gender equality;
- Art. 24: protection of the child and his right to life;
- Art. 25: the right of the elderly, with particular regard to special needs and care in terms of medical and bio-clinical care;
- Art. 26: the right of people with disabilities, with a particular regard to special needs and care in terms of medical and bio-clinical care;
- Art. 35: the right to a preventive healthcare system and to medical treatment, to grant the protection of human health;
- (I 1, 4): clinical research will be performed according to the moral principles for experimentation, and will be preceded by a careful assessment of risks;
- (II 2): combination of research and healthcare must be performed according to the therapeutic value for the patients;
- (III 4a): researchers must act in such a way as to safeguard the integrity of the individual, especially if the individuals condition and the information provided rely on the researchers performance.

Furthermore, all relevant legal sources (legislation, case law, studies, and surveys prior to legislation) at National and International level will be reviewed and examined thoroughly to identify the applicable policies and rules to be adopted. The sources considered for the purposes of this exercise include, but are not limited to European level:

- Art. 3, 7, 8 of the Charter of Fundamental Rights of the European Union;
- The Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

- Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use;
- Directive 2005/28/EC of 8 April 2005 laying down principles and detailed guidelines for good clinical practice as regards investigational medicinal products for human use, as well as the requirements for authorisation of the manufacturing or importation of such products;
- Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices;
- Art. 8 of the Convention of the Council No. 5 for the protection of human rights and fundamental freedoms;
- Convention No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data

Recommendations:

- Council of Europe, Recommendation No. R(97)5 on the protection of medical data adopted of 13 February 1997;
- Council of Europe, Recommendation on human rights and biomedicine, concerning biomedical research, Strasbourg 25th of January 2005.

Relevant International Instruments and Documents:

- UNESCO Universal Declaration on Human Genome and Human Rights;
- UNESCO International Declaration of Human Genetic Data;
- UNESCO Declaration on Bioethics and Human Rights.

No adverse side effects are expected from the experiments performed by SERUMS on patients or care staff that will make available their clinical and biological data, since the patient's care pathway and the solutions for the care staff, will be based on best practice and guideline recommendations, and results of the experiments will not affect the clinical decision-making during the duration of the project. The project will run according to the European legal and ethical requirements that will guarantee the compliance of researchers with the European Legal framework. As a fundamental principle underlying the project, the data subject himself is the owner of his data grants access to the data. Ethical and research governance will be required. Individuals unable to consent to participate will not be recruited. All data will be anonymised for processing; any personal data will be stored in a secure location separate from the anonymous data. USTAN will assume responsibility for public liability insurance, informed by a risk analysis process. All the medical and technical partners will have one person on call in case any incident should during the field testing period.

4.4 International regulation on ethics

The project will deal with highly sensitive healthcare data. Personal data processing requires a higher level of protection and is subject to numerous regulations. Furthermore, because of the therapeutic or scientific implications, such data processing has to absolutely minimize the potential of medical errors or erroneous scientific results.

- The Directive 95/46/EC of the European Parliament and the Council of the 24th October 1995 on the protection of individuals (with regard to the processing of personal data and on the free movement of such data);
- The European Group on Ethics in science and new technologies (EGE) report Citizens Rights and new technologies: a European challenge;
- Ethical issues of healthcare in the information society. Opinion of the European Group on Ethics in Science and New Technologies No. 13, 30 July 1999;
- Charter of the Fundamental Rights of the European Union, signed in Nice on the 7th of December 2000 (2000/C364/01);

- The World Medical Association (WMA) Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects;
- The principles ratified in the Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (Oviedo Bioethics Convention);
- The Ethical rules of the Horizon 2020 programme.

4.5 National Regulation on Ethics

The primary local regulations that need to be considered by FCRB in Spain are:

- Ley del paciente (Law of Patient), governing the use of patient data https://www.boe.es/buscar/act.php?id=BOE-A-2002-22188; and
- LOPD, regional governing data protection, http://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750.

As described above, these regulations will be fully complied throughout the execution of the SERUMS project.

The legislation and regulations concerning ethics in science, applied by ZMC in the Netherlands are:

- The Medical Research Involving Human Subjects Act[2] (Wet medisch-wetenschappelijk onderzoek met mensen (WMO));
- The Netherlands Code of Conduct for Scientific Practice[3], from the Association of Universities in the Netherlands.

The principles of the WMO and the Code will be applied, although these legislation and regulations, which are both based on the Helsinki Declaration[4]5 (DoH) drafted by the World Medical Association, although both are not fully applicable to SERUMS as it is not within medical research or research in which participants are subjected to specific behaviour. Within this context, the most important principles are: i) Scrupulousness; ii) Reliability; iii) Verifiability; iv) Impartiality; and v) Independence.

In the UK (USTAN) collection and use of personal data is regulated by the Data Protection Act 1998, which implemented Directive 95/46/EC on data protection (Data Protection Directive). Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) came into force across the EU on 25 May 2018. The General Data Protection Regulation will be applicable to the UK despite the UK's decision to exit from the EU. The following sectoral laws apply to the collection and use of personal data in the UK:

- Privacy and Electronic Communications (EC Directive) Regulations 2003.;
- Freedom of Information Act 2000;
- Investigatory Powers Act 2016.

In the UK, assurance of an appropriate balance between the protection of patient information and the use and sharing of information to improve patient care is overseen by the Independent Information Governance Oversight Panel. This body was set up at the request of the Secretary of State for Health in 2013 to monitor the implementation of the recommendations set out in the independent review of information sharing carried out by Dame Fiona Caldicott.

[2] http://wetten.overheid.nl/BWBR0009408

[3] https://www.vsnu.nl/files/documenten/Domeinen/Onderzoek/The_Netherlands_Code_of_Conduct_for_Scientific_Practice_2012.pdf

[4] WMA Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects. In: http://www.wma.net/en/30publications/10policies/b3/ acceded on 15.04.2015.

4.6 Participation in the SERUMS experiments

Participation of subjects in the research activities will be entirely voluntary and their informed consent will be requested in advance (opt-in informed consent). The necessity of an informed consent arises from the legislation and will be applied to end-users (primary and secondary) and informal caregivers. Both will sign two copies of the informed consent form, one for himself and another stored by the investigators. Such consent must be applied prior to the collection of data collection, and without it nothing can be processed, stored or transferred. These signed informed consent forms will only be available to the responsible evaluation manager, FCRB, ZMC and USTAN lead investigators, as appropriate. It will be destroyed at the end of the study. Informed consent material will be provided in written form. The "informed consent forms"" and the "Information sheets" will be written in language and terms understandable to the participants. Templates of these documents will be kept on file, together with the approvals/opinions of the relevant ethics committee and/or other competent bodies. Detailed information on the informed consent procedures in regard to data processing will be also kept on file. The project team involved will ensure that the participants understand all aspects related to possible privacy issues before the written consent is collected.

In order to achieve free and voluntary patient consent to participate in the specified project activities, SERUMS will:

- Define the SERUMS protocols for studies and validations/proof of concepts which will describe the aims of the research work, the methods that will be utilized, any possible conflict of interest, consortium details (e.g. affiliations of the researchers), the anticipated benefits and potential risks of the validation tests and the discomfort it could entail;
- Study participants will be provided with detailed 'Information Sheets' describing the aims, methods and implications of the research activities and their rights. The 'Information Sheets' will be written in a simple language to be understandable as more as possible. In particular, description of the data processing/ or the data collection/ or the study procedures will be provided to inform appropriately the study participants on the purposes of the study;
- Researchers conducting the specific research activities will meet with single participant in order to provide explanations and create legitimate motivation for the engagement;
- Ethics approvals will be requested from the Ethics Committees of the Fundació Clínic per a la Recerca Biomèdica (Spain), the Zuyderland Medisch Centrum (The Netherlands) and the University of St Andrews (United Kingdom), in the part of the research raising ethics issues through the preparation of protocols submitted to the Ethics Committees. Ethics approvals will be requested before the commencement of the part of the research raising ethics issues and copies of the approvals will be provided to the Research Executive Agency (REA).

While we will not specifically target vulnerable individuals/groups as research participants, and the participation of such individuals/groups is not essential for the purposes of the research that will be carried out, it is possible that they will nevertheless volunteer to participate in the research, e.g., as patients. All necessary steps will be taken to protect any vulnerable individuals/groups, including using data masking/cloaking to protect personal/medical/other sensitive data. Suitable ethics approvals will be obtained from relevant ethics committees, and all recommendations will be enforced.

The invited Participants will have the right via an informed consent and information sheets (see WP9 Deliverables):

- To know that participation in the research activities is voluntary;
- To ask questions and receive understandable answers before making a decision. The answers will be given in simple language according to the subject envisaged literacy;
- To know the degree of risk and burden involved in participation;
- To know who will benefit from participation;
- To know which data and how their data will be collected, processed, transmitted, protected during the project, and destroyed after the project;

- To withdraw themselves, and their data from the project at any time and without the need to give a reason;
- To know about any potential commercial exploitation of the research results.

Where necessary under the GDPR, host institutions will appoint a Data Protection Officer. Their contact details will be made available to all data subjects involved in the research. In other cases, a detailed data protection policy for the project will be kept on file.

5 Conclusions

This deliverable defined the technical challenges/requirements that should be addressed by the different tools/technologies, methods and techniques in the coherent SERUMS solution. The results have been fed into each of the technical work packages, forming a foundation for the design and implementation of the associated methods and tools. Furthermore, it defined the success indicators that will be used for measuring the SERUMS progress and impact. In particular, considering the use cases described in the D7.3 provided clear definitions of the Key Performance Indicators (KPIs), along with their corresponding metrics, as well as the Baseline and the Trial measurements that will be used for measuring the success indicators.

References

[1] Burr, W.E, Dodson, D.F., & Polk, W.T. (2006). Electronic authentication guideline. Technical report, National Institute of Standards and Technology.

[2] Shannon, C. (1949). A mathematical theory of communication. Bell System Technical Journal, 27, 379-423.

[3] Massey, J. (1994). Guessing and entropy. In Proceedings of the IEEE Symposium on Information Theory, IEEE Computer Society, 204.

[4] O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. In Proceedings of the IEEE, 91(12), 2019-2040.

[5] Komanduri, S., Shay, R., Kelley, P., Mazurek, M., Bauer, L., Christin, N., Cranor, L., & Egelman, S. (2011). Of passwords and people: Measuring the effect of password-composition policies. In Proceedings of the Conference on Human Factors in Computing Systems (CHI 2011), ACM Press, 2595-2604.

[6] Shay, R., Komanduri, S., Kelley, P., Leon, P., Mazurek, M., Bauer, L., Christin, N., & Cranor, L. (2010). Encountering stronger password requirements: user attitudes and behaviors. In Proceedings of the ACM Symposium on Usable Privacy and Security (SOUPS 2010), ACM Press, article 2 , 20 pages.

[7] Ur, B., Segreti, S., Bauer, L., Christin, N., Cranor, L., Komanduri, S., Kurilova, D., Mazurek, M., Melicher, W., & Shay, R (2015). Measuring real-world accuracies and biases in modeling password guessability. In Proceedings of the USENIX Conference on Security Symposium (SEC 2015), USENIX Association, 463-481.

[8] Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. 2015. SwiPIN: Fast and Secure PIN-Entry on Smartphones. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15). ACM, New York, NY, USA, 1403-1406. DOI: https://doi.org/10.1145/2702123.2702212

[9] Elizabeth Stobert and Robert Biddle. 2013. Memory retrieval and graphical passwords. In Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS '13). ACM, New York, NY, USA, Article 15, 14 pages. DOI: http://dx.doi.org/10.1145/2501604.2501619

[10] Constantinides, A., Belk, M., Fidas, C., & Samaras, G. (2018). On cultural-centered graphical passwords: Leveraging on users' cultural experiences for improving password memorability. ACM SIGCHI User Modeling, Adaptation and Personalization (UMAP 2018), ACM Press, 245-249. https://doi.org/10.1145/3209219.3209254

[11] Constantinides, A., Fidas, C., Belk, M., & Samaras, G. (2018). On sociocultural-centered graphical passwords: An initial framework. ACM SIGCHI Human-Computer Interaction with Mobile Devices and Services (MobileHCI 2018), ACM Press, 277-284. https://doi.org/10.1145/3236112.3236150

[12] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2012. How does your password measure up? the effect of strength meters on password creation. In Proceedings of the 21st USENIX conference on Security symposium (Security'12). USENIX Association, USA, 5.

[13] Maximilian Golla and Markus Dürmuth. 2018. On the Accuracy of Password Strength Meters. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18). Association for Computing Machinery, New York, NY, USA, 1567–1582. DOI:https://doi.org/10.1145/3243734.3243769

[14] Xavier De Carné De Carnavalet and Mohammad Mannan. 2015. A Large-Scale Evaluation of High-Impact Password Strength Meters. ACM Trans. Inf. Syst. Secur. 18, 1, Article 1 (May 2015), 32 pages. DOI:https://doi.org/10.1145/2739044

[15] Burr, W., Dodson, D., Polk, W. (2006). Electronic authentication guideline. Technical report, NIST

[16] Komanduri, S., Shay, R., Kelley, P., Mazurek, M., Bauer, L., Christin, N., Cranor, L., Egelman, S. (2011). Of passwords and people: measuring the effect of password-composition policies. In ACM CHI ’11, ACM Press, 2595-2604

[17] Microsoft Developers’ Blog. Signing in with a picture password. https://docs.microsoft.com/en-us/archive/blogs/b8/signing-in-with-a-picture-password

[18] Zhao, Z., Ahn, G., Seo, J., Hu, H. (2013). On the security of picture gesture authentication. In USENIX Security (SEC’13), USENIX Association, 383–398

[19] De Muro, P., Mazziotta, M. & Pareto, A. Composite Indices of Development and Poverty: An Application to MDGs. Soc Indic Res 104, 1–18 (2011). https://doi.org/10.1007/s11205-010-9727-z