Project no. 826278

SERUMS

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

Initial Requirements Analysis and Success Metrics for the Serums Technologies and Use Cases
D7.1

Due date of deliverable: 31st March 2019

Start date of project: 1st January 2019

Type: Deliverable
WP number: WP7

Responsible Institution: ZMC
Editor and editor's address: Cindy Wings (c.wings@zuyderland.nl)
Partners Contributing: ZMC, USTAN, ACC, IBM, SOPRA, SCCH, UCY, FCRB

Approved by:
Reviewers: Michael Roßbory (SCCH)
Vladimir Janjic (University of St Andrews)
Technical Manager: Juliana Bowles

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	07/01/2019	Cindy Wings (ZMC)	Defined TOC and added Executive Summary
V0.2	12/01/2019	Cindy Wings (ZMC), Ivo Buil (ZMC), Leon van de Weem (ZMC), Marios Belk (UCY), Andreas Pitsillides (UCY)	Added Introduction and defined SERUMS key challenges and overall technical requirements
V0.3	21/01/2019	Cindy Wings (ZMC), Ivo Buil (ZMC), Leon van de Weem (ZMC), Marios Belk (UCY), Elias Athanasopoulos (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)	First version of contributions regarding the Expected Impacts and Associated Success Indicators
V0.4	04/02/2019	Cindy Wings (ZMC), Ivo Buil (ZMC), Leon van de Weem (ZMC), Marios Belk (UCY), Andreas Pitsillides (UCY)	Updated Expected Impacts and Associated Success Indicators
V0.5	22/02/2019	Cindy Wings (ZMC), Ivo Buil (ZMC), Leon van de Weem (ZMC), Marios Belk (UCY)	Updates on the SERUMS key challenges and overall technical requirements
V0.6	04/03/2019	Cindy Wings (ZMC), Ivo Buil (ZMC), Leon van de Weem (ZMC), Marios Belk (UCY), Elias Athanasopoulos (UCY), Andreas Pitsillides (UCY), Euan Blackledge (Sopra), Michael Vinov (IBM), Wanting Huang (ACC), Michael Roßbory (SCCH), Santiago Iriso (FCRB), David Vidal (FCRB)	First version of SERUMS technologies technical requirements
V0.7	11/03/2019	Cindy Wings (ZMC), Ivo Buil (ZMC), Leon van de Weem (ZMC), Marios Belk	Updates on the SERUMS technologies technical requirements and on the expected impacts and success indicators

		(UCY), Elias Athanasopoulos (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)	
V0.8	22/03/2019	Cindy Wings (ZMC), Ivo Buil (ZMC), Leon van de Weem (ZMC), Marios Belk (UCY), Elias Athanasopoulos (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
V0.9	25/03/2019	Cindy Wings (ZMC), Ivo Buil (ZMC), Leon van de Weem (ZMC), Marios Belk (UCY), Elias Athanasopoulos (UCY), Andreas Pitsillides (UCY), Euan Blackledge (Sopra), Michael Vinov (IBM), Wanting Huang (ACC), Michael Roßbory (SCCH), Santiago Iriso (FCRB), David Vidal (FCRB)	Updates on the KPIs measurements for the evaluation of SERUMS success indicators
V1.0	27/03/2019	Cindy Wings (ZMC)	Final version of D7.1 provided to the deliverable reviewers for final review
V1.1	29/03/2019	Cindy Wings (ZMC), Ivo Buil (ZMC), Leon van de Weem (ZMC), Marios Belk (UCY), Elias Athanasopoulos (UCY), Andreas Pitsillides (UCY), Euan Blackledge (Sopra), Michael Vinov (IBM), Wanting Huang (ACC), Michael Roßbory (SCCH), Santiago Iriso (FCRB), David Vidal (FCRB)	Finalization of D7.1 based on the comments received from the reviewers and release of D7.1

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: Cindy Wings Email: c.wings@zuyderland.nl
Partner 3	**Accenture B.V.**
Contact Person	Name: Bram Elshof Email: bram.elshof@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: Euan Blackledge Email: euan.blackledge@soprasteria.com
Partner 6	**Université Catholique de Louvain**
Contact Person	Name: Axel Legay Email: axel.legay@uclouvain.be
Partner 7	**Software Competence Centre Hagenberg**
Contact Person	Name: Michael Rossbory Email: Michael.Rossbory@scch.at
Partner 8	**University of Cyprus**
Contact Person	Name: 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. Also, it defines a detailed description of the success indicators and 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.

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 identified use cases, 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 will provide 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

Table 1: Relationship to other SERUMS Deliverables

Deliverable	**Relation**
D3.1 (Report on Initial Differential Privacy Learning Models)	The initial requirements analysis and success metrics for the differential privacy learning models are described in this deliverable. A comprehensive report on the initial differential privacy learning models, as well as the initial description of the analysis framework and the obtained results will be provided in D3.1.
D4.1 (Report on Initial Data Fabrication and Semantic-Preserving Encryption)	The initial requirements analysis and success metrics for the data fabrication and semantic-preserving encryption are described in this deliverable. A comprehensive report on the initial data fabrication and semantic-preserving encryption, as well as the initial data masking methods for anonymization of medical data will be provided in D4.1.
D5.1 (Initial Report on Security Metrics and Authentication Policies)	The initial requirements analysis and success metrics for the security metrics and authentication policies are described in this deliverable. A comprehensive report on the security metrics and authentication policy designs tailored to the initial use cases will be provided in D5.1.
D7.3 (Initial Report on Use Cases and Evaluation)	The initial Key Performance Indicators, along with their corresponding metrics for the evaluation of SERUMS solution are described in this deliverable. The evaluation of the initial use cases, which will be based on the evaluation metrics reported in this deliverable, will be reported in D7.3.
D7.4 (Refined Requirements Analysis and Success Metrics)	The main technical challenges/requirements that the different tools/technologies, methods and techniques comprised in the coherent SERUMS solution, as well as the detailed description of the success indicators for the overall expected impacts are described in this deliverable. A refined version of the aforementioned will be provided in D7.4.

1.3 Structure of this Document

Following the current introductory chapter, the rest of the document is structured as follows. Chapter 2 describes the technical objectives and requirements of the SERUMS solution. Chapter 3 describes the expected impacts, along with the success indicators and the impact measurements.

2 SERUMS Technical Objectives and Requirements

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, the goal of the Serums project is to put patients at the centre of future healthcare provision, enhancing their personal care, and maximizing the quality of treatment that they can receive, while ensuring trust in the security and privacy of their confidential medical data.

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, functional and ethical challenges 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 the Description of Work (DoW), the main technical and functional requirements 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.

2.3.1 Personalized User Authentication (PUA) Tool

Personalized User Authentication is a knowledge-based user authentication scheme that aims to deliver personalized user authentication types (*e.g.*, textual, graphical) by considering each user's preference and interaction device, in order to achieve a viable equilibrium between security, privacy and usability.

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

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.

PUA 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

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	Develop support for non-relational databases.

4	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.

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.

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.

2.3.6 Distributed Ledger Technology (DLT)

Distributed Ledger Technology is used to is a new type of database system that maintains and records data in a way that allows multiple stakeholders to confidently and securely share access to the same data and information. Transactions or data are stored in a ledger that is distributed among interested parties that are participating in an established network of computers. A record of consensus is provided, using a cryptographic audit trail, which is maintained and validated by several individual users, called nodes, that independently check the data blocks. Only stakeholders that need to see the data will have access. And, if anyone tries to tamper with, duplicate or alter any part of the record, all stakeholders will know.

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.

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 (by at least 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 (by at least 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): • PUA will be based on user-adaptive and adaptable password policies • 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) **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

IBM Data Fabrication Platform (DFP):

- The technology will enable to test the Smart Healthcare systems on large volumes of synthetic, but realistic, data, both during development and during deployment to identify any potential vulnerabilities.

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: Online Guessability	**PUA**

Metrics:

This KPI will be measured using the following metrics:

- **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
- **Guessability:** Actual number of tries required to guess the password

Trial Measurements:

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]:

$$H_{max} = log_2 k_p \text{ [bits]}$$

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.

Guessability

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.

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 Practical Entropy and Guessability Measurements will be compared with the Trial Measurements. An increase in the Trial Measurement **Practical entropy** and **Guessability** 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, followed by video attacks. Therefore, we will show the shoulder surfers videos that will be cut to the password-entry. Per attack, a maximum

of three guesses will be allowed. Shoulder surfing attacks will be based on a one-time view of the input followed by three guesses. Video attacks will allow users unlimited control of the video. 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.

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** **DFP**

Metrics:

This KPI will be measured using the following metrics:

SPR:

- **System Vulnerability:** 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.

DFP:

- **System Vulnerability:** By providing high-quality synthetic data, the technology will enable to significantly improve the project system testing and thus reduce the risk of potential security vulnerabilities.

Trial Measurements:

SPR:

Verification of correct implementation: use of code analysis and understanding of the technology used to determine whether the system will have an increase in security

DFP:

Various types of penetration testing will be used to measure and demonstrate improvements in the security of the new Smart Health Center software.

Baseline Measurements:

SPR:

The baseline measurements will be the recording of the current state of system security. This will take into account the current method of authentication, the current patch version of the system, and the current state of the firewall and antivirus. We will use the hospitals' penetration test results as

the baseline for the attacks. If they have not already been done then we will carry them out

DFP:

The baseline measurements will be defined in the second version of this Deliverable (D7.4)

How Impact on the Success Indicator will be measured

SPR:

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.

DFP:

This will be defined in the second version of this Deliverable (D7.4)

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 (at least 75%), evidenced by quantitative metrics showing the

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 (at least 75%), 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

Personalized User Authentication (PUA):

- Through familiar images, users will select non-hotspots which will harden the guessability of selections on an image by a brute-force attack

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: Offline Picture Guessability	**PUA**

Metrics:

This KPI will be measured using the following metrics:

- **Picture Guessability:** Actual number of tries required to guess the picture password selections through an offline brute-force attack

Trial Measurements:

Picture Guessability

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.

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 Picture Guessability Measurement will be compared with the Trial Measurement. An increase in the Trial Measurement **Picture Guessability** value, implies a quantifiable (%) improvement in secure provision of health and care services.

KPI 2.2: 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.

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 2.3: Data Breaches	**SPR**

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 the use of the log files for the database 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. finance, physiotherapy, emergency, etc. Additionally, the audit trail that will be generated by the blockchain will allow accountability of who has accessed what. This will be recorded in a log file that we will be able to use as for comparison

Baseline Measurements:

The baseline will be measured by the volume of patient data that can be accessed by unauthorised members of staff or for inappropriate reasons in the current configuration of the system. This will be recorded via the log file of the database

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 log files from both the

baseline and trial measurements	
KPI 2.4: Enhanced Model Privacy	**PDA**
Metrics: This KPI will be measured using the following metrics: • **Metric:** Privacy of machine learning models will be measured using metrics like differential privacy, k-anonymity, etc. Furthermore, it will be measured based on the amount of data revealed using current privacy attacks like linkage reconstruction or inversion attacks.	
Trial Measurements: This will be defined in the second version of this Deliverable (D7.4).	
Baseline Measurements: Baseline measurements will be performed using state-of-the-art privacy preserving models.	
How Impact on the Success Indicator will be measured This will be defined in the second version of this Deliverable (D7.4).	
KPI 2.5: Data Integrity	**DLT**
Metrics: This KPI will be measured using the following metrics: • **Metric:** Time required to edit data on the ledger.	
Trial Measurements: Effort required to edit data with an unauthorised access to the DLT network via submitting new transactions. The length of time calculated using a predefined computing power under the condition that the strongest encryption algorithm was selected.	
Baseline Measurements: With identical predefined computing power, mathematically calculated time required to edit existing data with an unauthorised access to a traditional database technology that is being used in the current environment.	
How Impact on the Success Indicator will be measured Measurement in baseline should be exponentially higher than in the trial measurement. The attacker needs to hack majority of the nodes to create a new transaction and stored on the ledger. Time required exceeds the validity time of the data.	
KPI 2.6: Ability to discover tampered data	**DLT**
Metrics:	

This KPI will be measured using the following metrics:

- **Metric:** In the event of unintended data modifications by malicious party, Time needed to discover the data changes and restore the data. This requires to identify the specific data in question and the time to query the database/ledger in order to retrieve and restore the original value of the data.

Trial Measurements:

Time needed to discover and restore tampered data in the event of unintended data changes.

Baseline Measurements:

Time needed to discover event of unintended data changes and restore tampered data in the existing system. The result will be calculated based on understanding of the existing system and the current polices and functionalities in place.

How Impact on the Success Indicator will be measured

Time needed should be significantly shorter in Trial measurement. The probability to remove trace of such event should be exponentially lower thus it is less time consuming to retrieve the data in question.

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 (at least a factor of 2), evidenced by patient surveys and questionnaires.
- **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.

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 (at least 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

IBM Data Fabrication Platform (DFP):

- The technology will increase security and trust in the project medical software system, while at the same time decrease cost of the production, deployment and maintenance of such a system.

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.

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.

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:** Usability and User Experience 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.

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:** Usability and User Experience 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.

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.

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** **DFP**

Metrics:

This KPI will be measured using the following metrics:

SPR:

- **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.

DFP:

- **Surveys:** This will be defined in the second version of this Deliverable (D7.4).
- **Questionnaires:** This will be defined in the second version of this Deliverable (D7.4).

Trial Measurements:

SPR:

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

DFP:

Surveys

This will be defined in the second version of this Deliverable (D7.4).

Questionnaires (perceived trust)

Improved patient trust will be estimated through surveys, questionnaires and increased customers readiness to use the new Smart Health Center.

Baseline Measurements:

SPR:

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

DFP:

This will be defined in the second version of this Deliverable (D7.4).

How Impact on the Success Indicator will be measured

SPR:

The same questionnaire will be given to the original 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.

DFP:

This will be defined in the second version of this Deliverable (D7.4).

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

Metrics:

This KPI will be measured using the following metrics:

- **Metric:** Model utility measurements using benchmark datasets and comparison of state-of-the-art models with the models developed in WP3.

Trial Measurements:

This will be defined in the second version of this Deliverable (D7.4).

Baseline Measurements:

Baseline measurements will be performed using state-of-the-art models and benchmark datasets (e.g. MNIST)

How Impact on the Success Indicator will be measured

Higher utility of the models leads to better diagnostics thus resulting in higher patient trust

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:

- **Metric:** This will be defined in the second version of this Deliverable (D7.4).

Trial Measurements:

Metric

Model utility measurements using benchmark datasets and comparison of state-of-the-art models with the models developed in WP3

Baseline Measurements:

Baseline measurements will be performed using state-of-the-art models and benchmark datasets (e.g. MNIST)

How Impact on the Success Indicator will be measured

Higher utility of the models leads to better diagnostics thus resulting in improved patient safety.

4 Conclusions

This deliverable defined the main technical challenges/requirements that will be addressed by the different tools/technologies, methods and techniques in the coherent SERUMS solution. Furthermore, it defined a detailed description of the success indicators for the overall expected impacts through 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