Project no. 826278

# SERUMS

Research & Innovation Action (RIA)

**SECURING MEDICAL DATA IN SMART-PATIENT HEALTHCARE SYSTEMS**

# Report on Refined Use Cases and Evaluation of SERUMS Technologies in PoCs and pilots.

# D7.6

Due date of deliverable: June 30, 2022

Start date of project: January 1, 2019

Type: Deliverable
WP number: WP7

*Responsible Institution*: Zuyderland Medisch Centrum (ZMC)
*Editor and editor's address:* Larissa Haen-Jansen (la.jansen@zuyderland.nl)
*Partners Contributing:* FCRB, ZMC, USTAN, ACC, IBM, SOPRA, SCCH, UCY, UCL, UD

Approved by:
*Reviewers: Marios Belk (UCY)*
*Vladimir Janjic (UD)*
*Technical Manager: Juliana Bowles*

Version 1.0

| **Project co-founded by the European Commission within the Horizon H2020 Program** | | |
|---|---|---|
| **Dissemination Level** | | |
| PU | Public | X |
| PP | Restricted to other program 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 | 16-04-2021 | Ivo Buil (ZMC) | Create document, add structure and chapters, and add Use Case scenarios |
| V0.2 | 27-01-2022 | Ivo Buil (ZMC) | Add instructions and questionnaires to the Appendix |
| V0.3 | 13-05-2022 | Ivo Buil (ZMC), Leon van de Weem (ZMC), Julio Burgos (FCRB), Santiago Iriso (FCRB), Sascha van der Vliet (ACC), Emma Morley (USTAN) | Writing started for chapters 1, 2 and 3 |
| V0.4 | 17-05-2022 | Ivo Buil (ZMC), Leon van de Weem (ZMC), Sascha van der Vliet (ACC) | Format changed for chapters 3 and 4 |
| V0.5 | 24-05-2022 | Ivo Buil (ZMC), Leon van de Weem (ZMC), Sascha van der Vliet (ACC) | Checked and modified chapters 2, 3 and 4 |
| V0.6 | 30-05-2022 | Ivo Buil (ZMC), Larissa Haen (ZMC), Thais Webber (USTAN) | Revisions to use cases, checks for expect everything up till chapter 4, and added participant information letter |
| V0.7 | 15-06-2022 | Ivo Buil (ZMC), Leon van de Weem (ZMC), Larissa Haen (ZMC), Sascha van der Vliet (ACC), Julio Burgos (FCRB), Argyris Constantinides (UCY), Marios Belk (UCY) | Updating the PoC result and finalising the deliverable for a Silver Version |
| V0.8 | 28-6-2022 | Leon van de Weem (ZMC), Larissa Haen (ZMC), Sascha van der Vliet (ACC) | Update the document with review remarks and remove the track-changes |
| V0.9 | 29-6-2022 | Leon van de Weem (ZMC), Larissa Haen (ZMC), Sascha van der Vliet (ACC), Bram | Update the document with review remarks, finalise the document for submission. |

| Release No. | Date | Author(s) | Release Description/Changes made |
|---|---|---|---|
|  |  | Elshof (ACC), Julio Burgos (FCRB) |  |
| V1.0 | 30-6-2020 | Leon van de Weem (ZMC), Larissa Haen (ZMC), Sascha van der Vliet (ACC), Julio Burgos (FCRB) | Version for submission, final spelling check |

# SERUMS Consortium

| | |
|---|---|
| **Partner 1** | **University of St Andrews (USTAN)** |
| Contact Person | Name: Juliana Bowles<br>Email: jkfb@st-andrews.ac.uk |
| **Partner 2** | **Zuyderland Medisch Centrum (ZMC)** |
| Contact Person | Name: Larissa Haen-Jansen<br>Email: la.jansen@zuyderland.nl |
| **Partner 3** | **Accenture B.V. (ACC)** |
| Contact Person | Name: Bram Elshof<br>Email: bram.elshof@accenture.com |
| **Partner 4** | **IBM Israel Science & Technology Ltd. (IBM)** |
| Contact Person | Name: Michael Vinov<br>Email: vinov@il.ibm.com |
| **Partner 5** | **Sopra-Steria (SOPRA)** |
| Contact Person | Name: Andre Vermeulen<br>Email: andreas.vermeulen@soprasteria.com |
| **Partner 6** | **Université Catholique de Louvain (UCL)** |
| Contact Person | Name: Axel Legay<br>Email: axel.legay@uclouvian.be |
| **Partner 7** | **Software Competence Centre Hagenberg (SCCH)** |
| Contact Person | Name: Michael Roßbory<br>Email: michael.rossbory@scch.at |
| **Partner 8** | **University of Cyprus (UCY)** |
| Contact Person | Name: Andreas Pitsillides<br>Email: andreas.pitsillides@ucy.ac.cy |
| **Partner 9** | **Fundació Clínic per a la Recerca Biomèdica (FCRB)** |
| Contact Person | Name: Santiago Iriso<br>Email: siriso@clinic.cat |
| **Partner 10** | **University of Dundee (UD)** |
| Contact Person | Name: Vladimir Janjic<br>Email: VJanjic001@dundee.ac.uk |

# Table of Contents

# Executive Summary

SERUMS aims to increase the efficiency of healthcare systems in Europe while ensuring patient safety 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. To meet this challenge, SERUMS developed and implemented innovative methods, tools, and technologies (e.g., Blockchain, Data Lake, Data fabrication, Privacy preserving analytics, Personalised user authentication schemes) addressing the need for cybersecurity in hospitals including remote care and home-care settings. Through these developments, the SERUMS project expects to achieve a 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. In this document we will present this achievement.

The work, related to the demonstration of the SERUMS technologies' effectiveness on real-world use cases from the domain of using and analysing medical data, proceeded in three phases. The work performed during the first and second phase is presented in D7.3 and D7.5, respectively. The current deliverable (D7.6) presents the work performed during the third phase.

Looking back at the three Proof of Concepts, we see an improvement during each phase. In the first phase the integration of the SERUMS Technologies was not achieved yet. In the second phase an initial integrated and coherent version was implemented and tested. Last, the third phase showed a completed integrated system, where patients and staff evaluated against the final version of the use cases based on: i) the evaluation results of the second phase; and ii) extended with mechanisms for information sharing between patients, hospitals, local e-health providers, and other care organisations (GPs/paramedics).

To conclude, our findings show that we have achieved our initial proposed impact based on the Success Indicators, since all Success Indictors measured in PoC3 exceeded the benchmark values established. The specific KPIs helped us also identify areas that still have room for improvement. In the current state, the SERUMS system is not ready yet to be made available to the public, since not all exceeded the benchmark. Next steps (discussed in detail in D7.7 Report on Technical Roadmap for SERUMS Technology) include developing several functionalities to facilitate international data exchange and to facilitate hosting across multiple locations. It is planned to investigate alternative authentication methods for visual impaired users, such as audio recognition or other initiatives towards a more accessible authentication scheme, so the SERUMS system would be available to as many people as possible.

# 1 Introduction

## 1.1 Role of the Deliverable

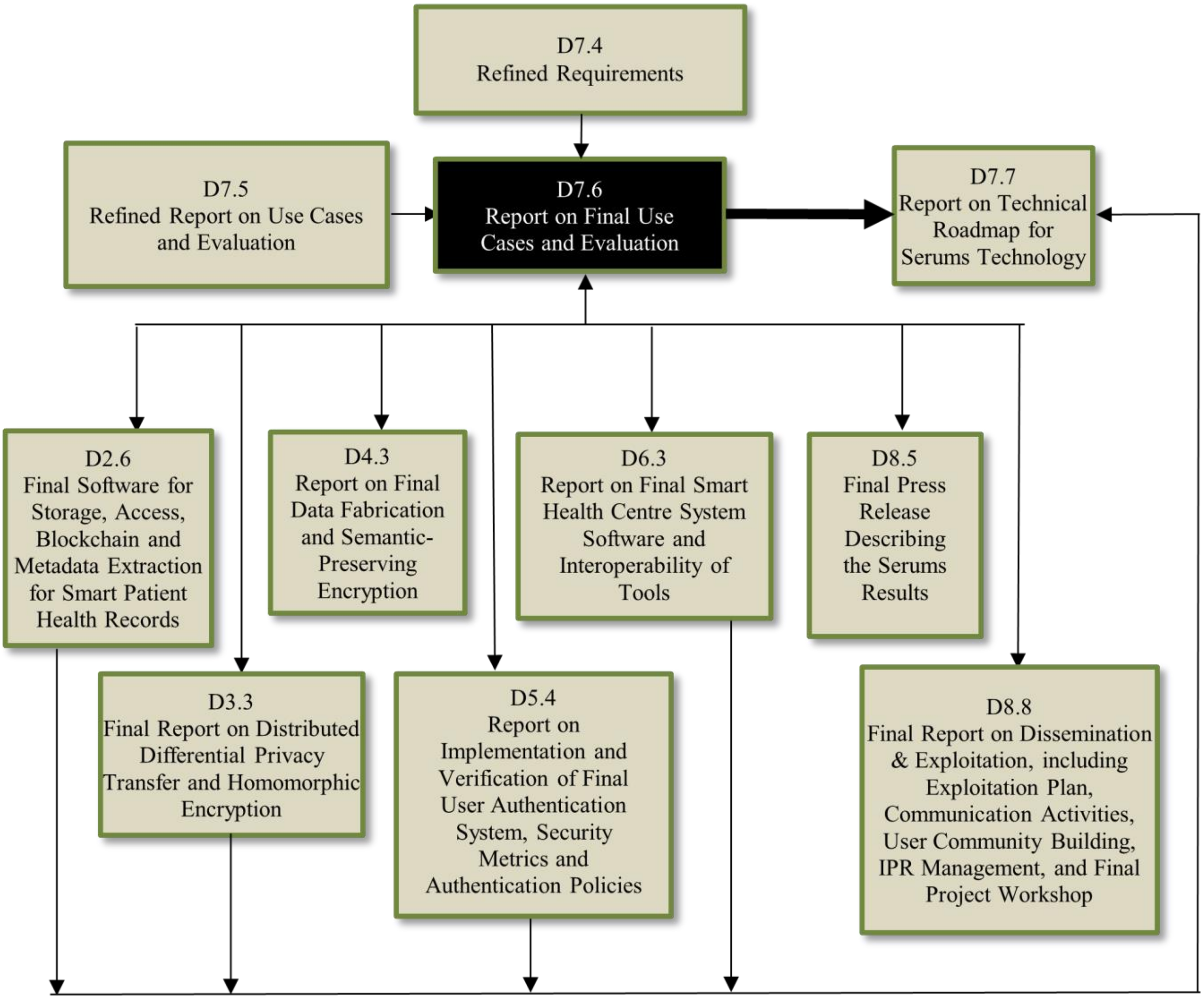
This deliverable aims to present the results of the work performed during the final phase of the demonstration of the SERUMS technologies' effectiveness. More specifically, this deliverable: i) defines a detailed specification of the final use cases, extended with mechanisms for information sharing between patients, hospitals/medical centres, local e-health providers and other caregiver organisations, that have been used for the final evaluation of the prototypes of the SERUMS technologies; and ii) evaluates the final prototypes of the SERUMS technologies developed, against the overall project requirements and success criteria that were identified in D7.4 and later refined after D7.5. During this phase, the focus is on completing the integration of all the SERUMS technologies, ensuring data ownership for all stakeholders/end-users within and between all medical centres in different European countries, educating end-users on the Proof of Concepts (PoCs) and Pilots, and measuring the progress aiming to reach the following impacts:

- Impact I = Quantifiable improvement in the secure provision of health and care services
- Impact II = Significantly reduced risk of data privacy breaches
- Impact III = Increased patient trust and safety

To measure the improvements, we established a benchmark for each KPI metric and Success Indicator. This enables us to determine whether the SERUMS technologies achieved the goals set out in the proposal.

# 1.2 Relationship to Other SERUMS Deliverables

The relationship of D7.6 (that builds on D7.5) with the other SERUMS deliverables is provided in the figure below:



D7.4
Refined Requirements
D7.5
Refined Report on Use Cases and Evaluation
D7.6
Report on Final Use Cases and Evaluation
D7.7
Report on Technical Roadmap for Serums Technology
D2.6
Final Software for Storage, Access, Blockchain and Metadata Extraction for Smart Patient Health Records
D4.3
Report on Final Data Fabrication and Semantic-Preserving Encryption
D6.3
Report on Final Smart Health Centre System Software and Interoperability of Tools
D8.5
Final Press Release Describing the Serums Results
D3.3
Final Report on Distributed Differential Privacy Transfer and Homomorphic Encryption
D5.4
Report on Implementation and Verification of Final User Authentication System, Security Metrics and Authentication Policies
D8.8
Final Report on Dissemination & Exploitation, including Exploitation Plan, Communication Activities, User Community Building, IPR Management, and Final Project Workshop

**Figure 1. Relations between deliverables.**

# 1.3 Structure of this Document

In Chapter 2 the Use Cases for the final Proof of Concept (PoC3) are discussed. Chapter 3 contains the executions of PoC3 by the end-user organisations. In Chapter 4 the evaluation of PoC3 and outcome of the SERUMS System is explained and in Chapter 5 Conclusions are outlined.

# 2 Use Cases Specification

This chapter provides a detailed description of the use cases that have been used for the evaluation of the final prototypes of the SERUMS technologies. The use cases described in this deliverable build on those described in D7.5 and extended with the criteria for international and emergency data sharing scenarios. Therefore, the final development phase of the SERUMS technologies contained additional requirements for each use case. In addition, the final phase focused on integrating all SERUMS technologies into a single, user-friendly, system. The final unified system uses realistic fabricated data from WP4 to build the data lakes in WP2 and visualises the toxicity predictors in WP3, by creating privacy-preserving data analytics models.

The ZMC Smart Health Centre use case (see section 2.1) describes a system in which all the medical data of a patient from hospitals, physiotherapists, and wearables is stored, and where the patient can manage which caregiver has access to which part of his medical data. This use case exploits: i) the smart patient records from WP2, ii) privacy-preserving and secure communication mechanisms from WP4 for gathering data from different devices, and iii) authentication methods from WP5. The system is based on the Smart Health Centre System that is developed in WP6. The use case is extended in this last period where the patient travels abroad and needs to visit the hospital there.

The FCRB use case (see section 2.2) consists of the HCB - Smart Platform (HCB-SP). Together with the help of the technologies developed during the SERUMS project, we intend to provide a patient an easy way to gather vital signs for the hospital using two wearable devices and the possibility to share them with all the professionals that care for them, even in emergencies abroad. As a use case, the HCB-SP exploits: i) the smart patient records from WP2, ii) privacy-preserving and secure communication mechanisms from WP4 for gathering data from different devices and iii) authentication methods from WP5. In the last period the use case is extended with the scenario that the patient needs emergency care, while visiting a friend abroad.

The USTAN use case (see section 2.3) mostly focuses on communication mechanisms for fetching the selected information to the central patient portal, displaying this information to the user, and creating anonymous predictive outcome values in the future based on the stored information. Therefore, this use case mostly exploits: i) mechanisms for smart patient records access from WP2, ii) privacy-preserving and secure communication mechanisms from WP3 and WP4, and iii) authentication methods from WP5. The use case is the same as in the previous period but emphasises the visualisation of the Smart Health Record.

## 2.1 ZMC - A New Hip

ZMC started the SERUMS project without any digital system with which patient data could be shared with the patient. The only way for a patient to acquire their medical records was to request a printable version of their records from the patient service centre[1]. Sharing medical data with other health care providers was thus only done through printable PDF files.

The aim of ZMC with the SERUMS project is to research, test, and develop a system that will be able to collect data from various sources and distribute them in a way that meets the criteria set up by the Dutch Government, GDPR, and patient expectations. This means that ZMC expects the system to be secure, user-friendly, meet all the privacy-preserving regulations, able to obtain/share medical data from/to a wide scale of sources, and distribute that data, accordingly, including hospitals, patients, wearable devices, external physiotherapists, and international clinics. We put a high emphasis on the correct use of blockchain and access/authentication rules. In addition, we encourage the use of only keeping the data at the original location, this way i) the original data cannot be tampered with through this system and ii) if a data breach does occur, not all the data is available in

[1] During this project ZMC implemented a web portal where patients can see parts of their medical data, without the possibility of sharing this data to other organisations.

one place. Furthermore, the use of real fabricated data is essential in the development phase, as we can then see the capabilities of the system without violating privacy regulations. Despite the demanding technical requirements, it is essential that the whole system will be extremely user-friendly, in such a way that patients do not run into age-related difficulties using the system. In preparation for the third PoC, the final integrated solution for the SERUMS system was ready and tested by our patients and caregivers. The IT personnel from ZMC were able to answer detailed questions on the system and give critical remarks to utilise the ideas and lessons learned for future releases / updates of our system. As mentioned before, this final integrated solution includes the updated business and technical requirements in section 2.1.2 which support cross-border data sharing extension of the user story. In addition, the final solution can show an individual's realistic fabricated health information, including fake PDFs and anonymised X-rays.

### 2.1.1 ZMC User Story

Peter is a 70-year-old male who has recently been provided with a new artificial hip at Zuyderland Medical Centre (ZMC). After a short stay at the hospital, Peter is dismissed and sent home to complete his recovery there. He can already view his medical data related to his injury and operations in his account at home in the Personal Health Environment (PHE) because he arranged that before the operation.

**Note**: The medical files in the hospital regarding basic characteristics, injury, X-rays, and operation details are easily accessible and compatible with the Personal Health Environment system.

Identification and authentication for sharing hospital data with the PHE needs to be done in a secure and user-friendly way according to the principles of the European General Data Protection Regulation (GDPR)[2] guidelines and so called MedMij[3] standards in The Netherlands.

To ensure Peter's recovery, the physician has ordered physiotherapy and the use of an Activity Monitor (AM) with an E-coach for 1 week. Before his surgery, Peter has already used the Activity Monitor, to measure his mobility before the hip replacement. The Activity Monitor is a precise instrument that measures if and how well a patient is active at a validated clinical level.

**Commentary**: To comply with the GDPR, Peter must provide explicit permission to:

- Specifically allow the Activity Monitor to provide his personal activity data to i) each medical practitioner that needs the results from it; and ii) the Smart Health Centre (SHC.)
- Specifically allow the E-Coach to share the guidelines that it provides with i) each medical practitioner that needs the results from it; and ii) the SHC.
- Allow each medical practitioner to share their medical records with the SHC, and vice-versa.

Under the GDPR, Peter may revoke any of these permissions at any time or choose to exclude some part of the information from being seen by any agent in the system, including historical information. However, doing this may be detrimental to his treatment, lead to false diagnoses, incur additional treatment costs, require him to take unnecessary drugs etc.

From the first session and the letter from the surgeon, the physiotherapist knows that Peter wears an Activity Monitor. He knows the results will tell him how stable Peter's condition is with his new hip. Together with giving Peter exercises he can do at home; the physiotherapist asks Peter if he will allow him to see all relevant medical files from the hospital and the results from the Activity Monitor. They agree that Peter will share the

[2] Information on GDPR can be found at https://gdpr-info.eu/

[3] Information on MedMij standards can be found at https://medmij.nl/en/information-standards/

files regarding the surgery and the daily results on the E-coach. Informed consent to share the data with the physiotherapist can be given via Peter's Personal Health Environment.

**Note**: Peter can choose in his Personal Health Environment which medical files and for how long he wants to share the medical files from the Hospital and the E-coach to the physiotherapist. The rights, rules, and communications of the data access will be ensured, logged, checked, and tracked via Blockchain.

Peter knows that the Activity Monitor needs charging every day. Because of its accuracy, it is an energy-consuming instrument and will last only 24 hours. Therefore, the nurse at the hospital explained to Peter that he needs to charge the battery every evening when he goes to bed. During charging, the measured data is transferred for analysis to show the results in the E-coach.

**Note**: The transfer needs to be secure. Data must be private and not tampered with. The raw data of the Activity Monitor is transported to an external server, where this raw data is analysed by a validated algorithm. Once the Activity Monitor receives a confirmation that the raw data is transferred successfully, it purges its data.

The results are available the next day to the physician via the E-coach and to Peter himself via his Personal Health Environment on his computer. Each morning Peter transfers the results from the Activity Monitor to the physiotherapist in his Personal Health Environment. Each day a trained nurse can then evaluate the stored results in the E-coach and can act accordingly.

**Note**:

1. Both the Activity Monitor and the validation algorithm do not know which patient is using which Activity Monitor. Yet in the E-coach and in the SHC, the link between the sensor ID of the Activity Monitor and the patient must be made. This is a potential danger for the patient when not done correctly.
2. The E-coach needs to send the results to the PHE in a secure way so that a patient cannot be identified during transport.
3. Identification and authentication in the E-coach or portal needs to be done in a secure and user-friendly way.

Data transport must be private and secure. The physiotherapist can now view the results Peter has sent them. The data transport is logged in Peter's record in the Personal Health Environment.

Peter finds it hard to get up from a chair or bed. He is afraid that his new hip will hurt him, causing him to use his muscles wrong and his first steps to be unstable. After a while, that feeling fades away, but the fear prevents him from exercising correctly. During his physiotherapy session on the fourth day, Peter is told that he should try to exercise more and that he needs to put more pressure on the leg with the new hip. The results have shown that Peter did not do his exercises and that when he gets up, he is not standing straight which might cause Peter to fall. Peter promises to improve his exercises. The physiotherapist can explain the effect of this to Peter from the graphical image of the results.

On the fifth day, the physician looks at the results of the last four days and concludes that Peter should have done better but sees an improvement on the fourth day. He tells the nurse to contact Peter and prolong the Activity Monitor until his 6 weeks follow-up session at the hospital.

**Note**: The extension of the Activity Monitor is administered in both the SHC and the E-coach and automatically visible in Peter's Personal Health Environment.

Peter improves his stability within the next four days. This is shown in the results of the Activity Monitor. The physician acknowledges this improvement and orders a digital consult with Peter for his standard 6-weeks follow-up. There is no need to see him physically. Peter will be asked to transfer the data from his physiotherapist to his physician when his physiotherapy has ended. Peter agrees and transfers the physiotherapy journal to his Personal Health Environment for the physician.

**Note**: This is administered in SAP. The request for sending the data from the physiotherapist is automatically visible in Peter's Personal Health Environment in a secure and private way.

Peter transfers in his Personal Health Environment the journal from his physiotherapist to his physician in a private and secure way. He has control over the timing and content of this transfer.

## 2.1.2 ZMC User Story - Addition to PoC3

A few weeks after his operation, Peter goes on holiday to Barcelona where he wants to explore the city and visit different neighbourhoods. After a few days of walking around, Peter notices that his hip starts to hurt. On the 5th day, the pain has only gotten worse, and since his operation was not long ago, Peter worries. He goes to the local hospital clinic (FCRB) for a consult. Peter explains his complaints to the physician and tells him that he has recently received a new hip. He is happy to share his medical data from the Netherlands with him. The doctor is pleased that Peter uses the SERUMS technology. Peter allows via SERUMS that the doctor in Spain can see his necessary medical details.

**Note**: When a new patient enters a hospital, a **blank slate** is created in the hospital for his medical data. The patient can then receive a SERUMS Name and ID from the department of the hospital which he can use to create an **access rule** for that department. The patient can decide for himself what is **relevant data** to share. When granted access, the department can view the shared medical data, but not integrate it directly into their hospital system.

The doctor in Spain evaluates the orthopaedic reports and the results from the Activity Monitor and sees no abnormalities. He examines Peter walking and concludes that Peters' hip is hurting because he is constantly walking on flip-flops. The doctor checks his drug intolerance, which only relates to iodine. He prescribes a painkiller and gives the advice to wear normal shoes. His complaints are gone a few days later. The doctor asks Peter to share his findings with his physician and physiotherapist via SERUMS. Peter logs in and allows his physician and physiotherapist in the Netherlands to view the data from Barcelona.

**Note**: For data to be shared between each care organisation, the patient must create new access rules that gives the care organisation in the Netherlands access to the data from FCRB.

**Note**: All full reports are in the local language. However, operation details such as anatomic location, laterality and resources are standardised and readable. Luckily most medical terms are in Latin.

Two weeks before the annual check-up, Peter is invited to the hospital for an X-ray of his hip and again receives the Activity Monitor and the E-coach from ZMC to monitor his recovery for 1 week. The results of the weekly AM and X-Ray are positive. The physician orders the physician assistant to have a digital consult with Peter, as it is not necessary to see him physically.

## 2.1.3 ZMC SERUMS system requirements

The table below shows which challenges or needs arise in the ZMC use case, what solutions need to be implemented and which technical implications it gives[4].

| No. | Challenge /Need | Solution | Remarks/Notes | Technical Implication |
|---|---|---|---|---|
| **1** | **Under GDPR** | | | |
| a | Peter's health data must be filling up in the personal health environment | Peter's Health environment is connected to Peter's health organisations to which data is sent or can be retrieved on the fly. | Aside from his health data, when applicable, this includes the names and roles of the designated Care professional per organisation. | **Smart Patient Health Record:** This is a centralised data source that allows all the patient's records to be accessed from a single source, regardless of the source system |
| | | *Peter's Health environment clearly visualises medical data from different caregiver organisations/hospitals/third party wearables, and divides these into categories.* | | ***Smart Patient Health Record**: The centralised data must contain multiple types of IDs to distinguish the caregivers, organisations, and categories of data.* |
| b | Peter must be able to connect any external device and E-coach he wants | The results from the Activity Monitoring E-coach can be shared with Peter's Health environment | | **Smart Patient Health Record:** The structure of the record allows for seamless integration of any additional data sources |
| c | Peter must be able to log in with the method and options he prefers | Peter logs in to his Personal Health environment using Picture Guessing. | All types of his preferred authentication methods (e.g., graphical password or textual password, Two-Factor Authentication) need to be accessible | **Personalised User Authentication:** Based on the suggested flexible and personalised authentication approach, end-users have the option to choose their preferred authentication method (*i.e.*, graphical, or textual) to login.<br>After successfully entering the password secret, for adding an additional layer of security, a push notification is sent to the end-user's mobile device that (s)he needs to |

[4] The update to these requirements is presented in Italic font.

| No. | Challenge /Need | Solution | Remarks/Notes | Technical Implication |
|---|---|---|---|---|
| | | | | approve to complete the login process. After successful completion of the login process, the authentication system generates a security token (JWT) and sends it to the client that is used for subsequent requests to the SERUMS systems. |
| d | Patients need full control over which data is sent, to who (and who not), and for how long. | Peter sees in his Health environment a special page with all currently active data access rules, which he can modify or remove at any time. On this page, Peter selects to create a new access rule. | The view can be the other way around. Peter selects an organisation or Care professional and then looks at which data is shared with that organisation. In the end it all comes down to Care professional → permissions ← data. It is a n to m relation<br>The same way sharing data is allowed, so is revoking sharing the data. | **Blockchain:** The default permission for the caregiver to access the patient is defined by the hospital administrator. Patients have the possibility to view existing rules, create additional rules to permit or restrict access for a selected set of data and to modify or delete an existing rule. |
| e | | Peter can the select which type or rule and which organisation, department or individual he wants to create a new rule for. Peter chooses to create a new rule that allows the entire external physiotherapy organisation access or a hospital abroad to certain Peter's Health data. | *When creating an individual rule, the list of caregivers must never be shown for privacy reasons. Peter must write down the correct name in a text field*<br>. | **Blockchain:** The structure of the blockchain contains IDs to identify caregiver organisations, caregivers, and patients. In addition, it contains information on the categories and source of the data that is being granted/denied access. |
| f | | Peter then sees a list of data categories he can give access to. Peter selects the wearable category from the list | | |
| g | | Peter now has the option to choose a certain period he wants to share his Activity Monitor data. Since Peter only uses the Activity Monitor for a week, Peter chooses this time frame for | | |

| No. | Challenge /Need | Solution | Remarks/Notes | Technical Implication |
|---|---|---|---|---|
|  |  | sharing. Furthermore, he checks all data to be shared |  |  |
| h |  | Peter needs to confirm this request for sharing and is then led back to the page where he can see in health data and if it is shared, partly shared, or not shared |  | **Blockchain:**<br>Patient's confirmation triggers the creation of the rule to allow the caregiver specified in the rule to access his data. |
| k | Setting specific documents to be shared | Some of the medical data from the hospital contains subsets of data. Peter can choose whether he wants to share all data or specific data. Peter selects his hip operation details. | Since this a specific part of the data and a single document no time frame will be asked. | **Smart Patient Health Record:**<br>The record stores data in a Data Vault structure, wherein only highly correlated data is stored in the same satellite. This works in conjunction with the Blockchain to ensure granular control over the access |

**Table 1 System requirements for ZMC User Story**

# 2.2 FCRB - Chronic Disease Management (HCB-SM)

With the new strong need of securing data and the GDPR, the Hospital Clinic de Barcelona is in a strong need of innovations in its ICT infrastructure. This is especially true in terms of having the patients in control of their data, since this is a total change of how their data has been managed traditionally. Whereas now the patient has only been able to request it when needed in case that the data was needed to receive treatment in another health centre not included in the Catalan Public Health System. In addition, the increase in data leaks from health organisations has made the need for new secure systems scale to maximum priority.

These two urgent needs are expected to be satisfied during the SERUMS project. On one side FCRB expects a practical proposal on the access permit management by ACC since an implementation would mean a dramatic improvement in our organisation. On the other side, as the times of Big Data and Artificial Intelligence demand an improved data organisation of the patient record and all the Hospital data in general FCRB is interested in how SOPRA manages to create their Data Lake.

Finally, on the side of UCY's Proposed Authentication Scheme, FCRB is indeed interested in if it represents an improvement over the habitual passwords in security and usability, but it will have to prove that the system will help old people to interact with the Hospital systems since they are the bigger proportion of the population in the Catalan Health Assistance.

Although the technologies will be integrated into the Smart Health Centre System, FCRB and the Hospital Clínic de Barcelona intend to integrate the SERUMS technologies to create a patient-oriented distributed system of their own. This new system will allow the Hospital patients to upload data gathered by e-health devices that can be taken home, allowing them to monitor patients with multiple chronic diseases. Section 2.2.1 presents the user story that this system plans to satisfy.

On the other side, the Privacy-Preserving Data Analytics is a completely new approach to security that at Hospital Clínic de Barcelona has never been considered. Nevertheless, with this project we hope that SCCH does a great job of showing its advantages and novel features over the more traditional approaches.

In preparation for the third PoC during the final phase of the evaluation, the integrated solution was improved by including mechanisms that allow the real fabricated data to be shared between organisations in other European countries and to make sure that the patient can only give access to trustworthy sources. To meet this additional requirement, additional steps have been included in section 2.2.2.

## 2.2.1 FCRB User Story

Joana is an 85-year-old female with several chronic diseases: she has diabetes and chronic heart failure (for which she receives medication). Joana lives in a private apartment close to a Primary Care Centre. She is getting some care via the Primary Care Centre but wants to remain independent for as long as possible. For that reason, her doctor, from the Hospital Clínic de Barcelona, a specialist in Diabetes, has given her wearable medical devices: i) a wireless pulse oximeter, to monitor her oxygen blood percent and her cardiac frequency; and ii) a wireless glucometer to measure her own glycemia.

**Note**: The following sensors will be made available to the health professionals to give to the patients:

- Pulse oximeter
- Glucometer
- Thermometer
- Tensiometer

All these devices will connect wirelessly to a smartphone application through Bluetooth 5 in a secure way.

**SERUMS Interaction**: The user will gain access to the HCB-SP through the authentication system provided by UCY, which frontend will be embedded in the Patient application and Professional platform.

For the second device, Joana has been informed that she will have to periodically upload her glycemia and oxygen in blood results to the HCB-SP platform through a mobile phone application called Saludata which basic usage has been taught by the doctors.

**SERUMS Interaction**: All information concerning patient record data and the measurements taken by the eHealth devices will be securely stored on the Data Vault provided by SOPRA. None of the HCB-SP will ever store personal data, these will always be retrieved from the Data Vault when needed.

Joana is happy with this because she can control her progress in this matter. With this smartphone application, Joana is totally in control of the data generated by the devices and her patient record. Joana has therefore given the doctor her permission to access her data on that platform.

**SERUMS Interaction**: The access and modification permissions over the patient data will be stored in the Blockchain solution developed by ACC. This will include various levels of information access, from only accessing the Patient Record to the granular access to only the information related to an aspect of the Record History (e.g., Endocrinology Record, Surgical Operation, etc.)

The Doctor commented to Joana that her General Practitioner needs access to the glycemia web portal to monitor her evolution and he will contact her to follow up on that and on the rest of her health issues.

**Note**: The Blockchain solution is not only for personal permission and professional but also for departments, organisations, and for the whole hospital.

In addition, more complex rules can be generated by Joana or the Hospital administrators.

**Explanation**: The Saludata application is to be in full compliance with the GDPR and thus must provide:

- Full control of who can access the patient data.
- Full control of which parts of the patient record each hospital, professional, or service can access.

On the other side, a cardiology medical team oversees taking care of her chronic heart failure and is composed of two nurses and one cardiologist. One of their tasks is to monitor the evolution of the patients with chronic heart failure at home, they receive and monitor all the data generated by the wireless pulse oximeter through an application installed on local servers of the hospital, where they can review Joana's list of measurements and communicate with her through notes with her smartphone app if necessary.

The hospital nurse periodically generates clinical notes with the events that have occurred and sends them to the patients. With this information and the glycaemic control from Joana's device, the General Practitioner can (with Joana's approval) collaborate to monitor, control, and detect abnormalities not only in one of those two diseases but can merge all of Joana's health issues and provide her with a better quality of life, by taking a holistic approach of her health status.

In terms of the technical flow of the use case, first, the patient will be told by the hospital or their caregivers to download a Smartphone application to communicate with the eHealth Devices and with the Central System. Patient's devices will be connected to the application in a secure standard way and all the health data generated for this application will be stored in the Central System's Data vault. Besides, the application can retrieve the history of personal health measurements, grant or revoke permits to the professionals, groups, or caregivers stored in the blockchain and send notes to them in a secure way.

The HCB-SP will have a second part that will be used by the caregiver to retrieve and review patient data to which it has given permits and send notes in the case it is considered necessary. As the smartphone application, this system communicates with the Authentication System, the Blockchain solution, and the Data vault to perform adequately. Nevertheless, this platform will not be installed in the user system but will be integrated with our Information Communications and Technologic Systems (ICT) and will be presented to the patient as a web application only accessible through the Hospital Network.

Both systems will communicate with the Central System provided by the SERUMS project using the Authentication Schema (UCY) and retrieve and store data from the Data Vault (SOPRA) depending on the permits each user has on the Blockchain Solution (ACC).

### 2.2.2 FCRB User Story – Addition to PoC3

In the summer, Joana has decided to visit a friend in Amsterdam. Her doctors have recommended that she takes her wearable medical devices with her, and so she has. On one of the days, she and her friend take a boat trip through the canals of Amsterdam. Halfway through the trip, Joana becomes unwell, and an ambulance is called to bring her to the hospital. During the ambulance ride, Joana informs the ambulance personnel that they can use her SERUMS ID card in her wallet to gain access to her medical files. The emergency room physician requests the patient's medical data through the emergency protocol in SERUMS using the identification number on the card. Joana accepts this emergency access using the secondary authentication system. Both nurses and doctors from the hospital's emergency department can now view all of Joana's medical records, and this access is indisputably registered in the SERUMS system.

**Note 1:** During an emergency, all available medical data is shared with the care organisation for a limited amount of time. It is possible to opt-out of the sharing of medical data when a non-treatment declaration is signed.

**Note 2:** The emergency access is recorded in the patient's Patient Record and can thus be viewed by the doctors in Spain.

The emergency personal notices that Joana has diabetes, and that they can see the most recent results from her wireless pulse oximeter and wireless glucometer. Here, they notice that the wireless glucometer measured a low glucose level. After double checking that her glucose levels are insufficient, the emergency doctors can treat her accordingly. After treatment, she can recover that same evening. The doctors in Amsterdam can help Joana adjust the insulin dosages for the rest of her vacation and if she regularly checks her glucose values, she should be able to enjoy the rest of her vacation. The emergency personnel make sure that the medical records created in their hospital system can be accessed by Joana in SERUMS and her caregivers in Barcelona. Joana can then create an access rule for her doctors in Spain to see what happened to her.

### 2.2.3 FCRB SERUMS system requirements

The table below shows which challenge or needs arise in the FCRB use case, what solutions need to be implemented and which technical implications it gives.[5]

| No. | Challenge /Need | Solution | Remarks/Notes | Technical Implication |
|---|---|---|---|---|
| **1** | **Vital Sign Monitoring** | | | |
| a | The health professionals need to have all the vital signs stored in only one platform. | The Saludata smartphone application would gather all the measurements from different devices in only one platform facilitating a complete monitoring of the patients. | Professionals often find themselves having to access multiple platforms from different vendors and devices | **Smart Patient Health Record:**<br>This is a centralised data source that allows all the patient's records to be accessed from a single source, regardless of the source system |
| b | The ability to have a periodic stream of vital sign data from chronic disease patients would greatly help the health professionals to treat them | The Saludata smartphone application for patients can read vital signs measurements and store for review or for the professionals to see them. | | **Personalised User Authentication**:<br>patient and professional must be authenticated and thus in possession of their security token (JWT), that will be used to utilise all the other technologies<br>**Blockchain**:<br>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.<br>**Smart Patient Health Record**:<br>The data will be retrieved from this system and sent to the end-systems in a secure way using SFTP |

[5] The update to these requirements is presented in Italic font.

| No. | Challenge /Need | Solution | Remarks/Notes | Technical Implication |
|---|---|---|---|---|
| **2** | **Improvement in Security** | | | |
| a | Data exchanged between health assistance actors and patients' needs to be secure. | In the whole platform securely communications, storage and access will be enforced | This includes each element in the communication chain or any component with which the system has relation | Smart Patient Health Record:<br>When a rule is successfully triggered on the Blockchain, the corresponding set of data will be moved to a secure location in the Data Lake and encrypted by a unique public key provided by the request. Once it is encrypted, it can be passed to the SERUMS system, with only the correct private key allowing the decryption |
| **3** | **In compliance with the GDPR compliance and data protection** | | | |
| a | Joana needs to be able to grant and deny access to her data to the distinct actors in their health assistance (doctors, nurses, hospitals, services, etc.) This includes organisations abroad. | Through the Saludata application Joana will be able to create and eliminate these permits, allowing her to manage granular access to her patient record. | | **Personalised User Authentication**: patients and professionals must be authenticated and thus in possession of their security token (JWT), that will be used to use all the other technologies.<br>**Blockchain:** Permission rules to grant or restrict access can be defined by the patient for health organisations, individuals, or groups. |
| b | | Joana can remove access to certain professionals or assistance services that are part of an allowed organisation. | | **Blockchain:** 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. |
| **4** | **Improvement in Patient-Health Assistant communication** | | | |

| No. | Challenge /Need | Solution | Remarks/Notes | Technical Implication |
|---|---|---|---|---|
| a | Communication between professionals and patients would be beneficial in the treatment of chronic diseases. | Both the patient application and the professional platform allow us to exchange messages through secure channels. | | |
| ***5*** | ***Creation of emergency personnel*** | | | |
| *a* | *In case of emergency, selected emergency staff must be able to easily obtain a patient's medical information* | *The administrator a care organisation can select medical personnel with emergency tags that allow them to more easily request all medical data based on patient-ID or SERUMS-ID.* | *The patient still needs to accept this request.* | ***Smart Patient Health Record**:*<br>*Medical personnel with emergency tags must be created. These tags can be activated or deactivated by the admin user of a care organisation* |
| *b* | *Safeguards must be in place to protect against misuse of the emergency clearance* | *The system must be able to track who uses the emergency clearance and on which patient, so that, if necessary, appropriate actions can be taken to prevent misuse* | *The patient should receive a message when an attempt is made to gain access through an emergency protocol* | ***Blockchain**:*<br>*An end point is provided to access the activity log which include the activities such as emergency/ other abnormalities.* |

**Table 2 System requirements for FCRB User Story.**

## 2.3 USTAN - Chemotherapy Toxicity Predictor

There are always ways in which healthcare provision can be enhanced, particularly concerning the management and treatment of highly complex chronic conditions such as cancer. Such conditions can give rise to further complications particularly in the case of elderly patients who may be frail and have additional comorbidities. For this use case, we consider breast cancer patients with comorbidities and undergoing chemotherapy. These patients only come to hospital for chemotherapy treatment approximately every three weeks and stay at home between treatments. As long-term research collaborators with the University of St Andrews, the Edinburgh Cancer Centre (ECC) and the Western General Hospital (WGH) within NHS Lothian[6], have an interest in exploring the use of technological solutions to improve the monitoring of the wellbeing of patients at home, and detect any changes in symptoms and side effects that need to be controlled. The vision of this use case is to add a way for patients to record symptoms daily whilst at home and send their data to the hospital and their registered medical practice so that the team at the WGH and the patient's GP can monitor and intervene as necessary. Interventions may be necessary if symptoms are indicative of high toxicity levels and bad reaction to the treatment received. The way that patients share data with the medical institutions from their home should be done securely and preserving the confidentiality of the data. The data can be further integrated with the treatment information to predict further evolution and compare patient outcomes with cohorts of similar patients more accurately. Furthermore, giving digital solutions to patients makes them more involved with their own treatment and health which could help in changing the perception of cancer treatments in the future. In addition, the ability to fine tune treatments to individuals is a trend within personalised medicine.

We proposed the development of a dashboard to help doctors (oncologists) observe, monitor, and analyse the condition of their patients over time. It can be used to analyse the effect of different chemotherapy treatments when given to patients with similar characteristics, and consequently influence future decisions to improve the well-being and survival rate of patients. Our aim is to deliver a system to predict the toxicity of chemotherapy treatments based on medical records and recorded feedback from patients over time. The overall features of the envisioned system for the NHS are illustrated below.

[6] https://www.nhslothian.scot

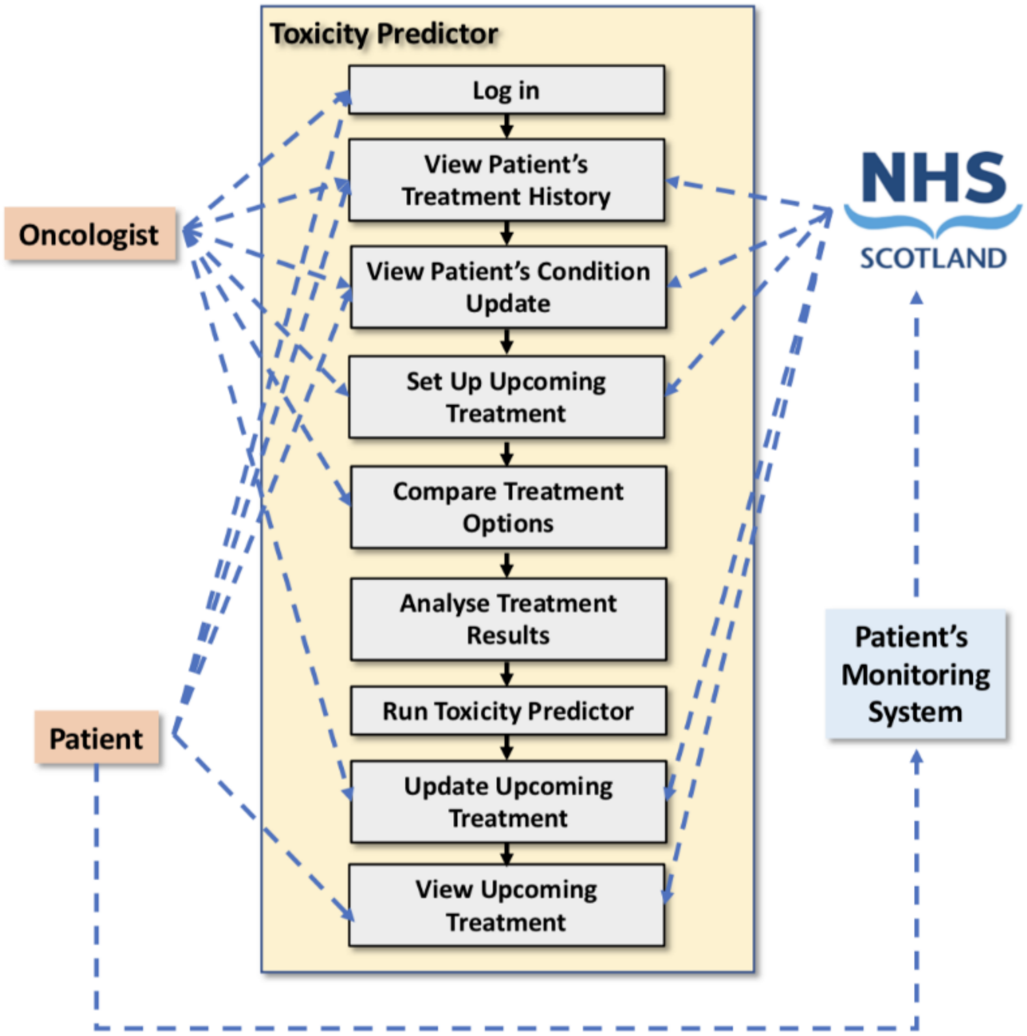

Toxicity Predictor
Log in
View Patient's Treatment History
View Patient's Condition Update
Set Up Upcoming Treatment
Compare Treatment Options
Analyse Treatment Results
Run Toxicity Predictor
Update Upcoming Treatment
View Upcoming Treatment
Oncologist
Patient
NHS SCOTLAND
Patient's Monitoring System

**Figure 2. Toxicity predictor system design USTAN**

There are two main topics for USTAN's use case within the SERUMS project. The first one is for the creation of a chemo care toxicity predictor which uses fabricated data from the IBM Data Fabrication Platform (WP4), which can be visualised in the frontend of the Smart Health Centre System (SHCS) within WP6, through various backend interactions involving further components within the system as required (authentication, data lake, blockchain, and so on).

The development of models for the toxicity predictor from large, fabricated datasets based on USTAN's use case enables the analysis and testing of the different techniques and methods in machine learning applications, which can help, for example, predicting outcomes for cancer patients and guide doctors towards better clinical decisions during treatment cycles.

This second topic of the USTAN dataset is the evaluation of the privacy-preserving machine learning approach developed by SCCH (WP3).

## 2.3.1 USTAN User Story

Emma is a 38-year-old patient in the Western General Hospital (WGH) who has recently been diagnosed with breast cancer. To prevent the spreading of the tumour, she underwent breast surgery. After her surgery, chemotherapy treatment is given as a follow-up to her surgery. She is now dismissed and only visits the hospital for her chemotherapy appointments every three weeks.

To ensure her wellbeing and best outcomes, and to be sure that the treatment plan is suitable and minimises further side-effects and further hospitalisations, a treatment plan and regimen have been established (this will be over several months with treatment in the hospital every three weeks). Emma has comorbidity. As any cancer patient on chemotherapy, she might have higher toxicity levels as a result, but it is crucial to guarantee that the scale does not go above level three. Toxicity levels range from 0 (no toxicity) to 5 (very high toxicity).

Emma agrees on using and sharing data between treatment visits via the cancer data gateway and patient portal. Emma determines who in the medical team sees this information: The oncologist/nurse and her GP. Emma is informed about how to use the web application and pass on relevant information to the clinical team.

Emma can provide information on symptoms periodically throughout the treatment. Patient Reported Outcome Measures (PROMS) within hospitals are based on questionnaires. Severe reported symptoms can be picked up by the clinical team and acted upon as soon as possible.

**Note**: The conditions that are being monitored and provided by the patients are nausea, vomiting, diarrhoea, constipation, oral mucositis, oesophagitis, neurotoxicity, hypersensitivity, and fatigue. With these symptoms, the oncologist can determine the level of patient toxicity.

The information Emma provides on her condition together with cancer information, hospitalisation data, and information about comorbidities, are all combined.

This combined data will help clinicians adapt treatments better to Emma as an individual patient which results in controlled toxicity levels and improved health outcomes. It uses data from several patients treated over the years with comparable characteristics.

If during the treatment there are signs that toxicity levels are high or that Emma’s condition is deteriorating, one of the members of the clinical team (e.g., oncologist, specialist consultant, nurse, GP) will identify the irregularities in Emma’s data, and contact Emma to intervene.

During a phone call, a decision is made for the GP/nurse to visit Emma at home and provide some additional medication to alleviate symptoms. Admission to the hospital is not necessary. As scheduled, Emma comes to the WGH for the next chemotherapy treatment. This procedure is iterative until the end of the chemotherapy treatment.

Overall, Emma can have more personalised treatment. If a complication arises, the clinical team can act more quickly. Furthermore, Emma’s well-being increases as she gets more involved in her treatment plans.

## 2.3.2 USTAN SERUMS system requirements

The table below shows which challenges or needs arise in the USTAN use case, what solutions need to be implemented and which technical implications it gives.

| No. | Challenge/Need | Solution | Remarks/Notes | Technical Implication |
|---|---|---|---|---|
| **1** | **More personalised treatment with improved and more regular monitoring of side effects. This will enable the clinical team to act more quickly when complications arise.** | | | |
| a | The oncologist needs to be able to observe the patient's condition before giving them the next chemotherapy treatment. They can see the medications prescribed by the GP for other diagnosed conditions as well. Some of the information is not accessible by the oncologist as it is held by the system of the medical practice. | A data sharing system allows the doctors (e.g., oncologists) to observe the latest patient's toxicity/condition measurement results. In addition, information on medication and dosages currently being taken and for what conditions is shown. | The oncologist may need to access multiple platforms for monitoring the patient's condition. | **Smart Patient Health Record**:<br>This is a centralised data source that allows all the patient’s records to be accessed from a single source, regardless of the source system. This will work as an extension for the SESO Gateway system. |
| b | Streamline the process of providing information on the patient's condition between hospital visits. | A monitoring application within the healthcare provider allows the patient to give an update on their symptoms at any given time, and anywhere. Patients can input their condition, and the data is directly collected and stored in their database. | A data sharing system with direct access to the information in the hospital database. | **Smart Patient Health Record:**<br>The SERUMS Data Lake will maintain a tagging system (the available patient metadata - SPHR) to acquire the patient information every time a request is issued by patients or medical professionals. |
| c | The oncologist requires/needs tools that provide insights on the upcoming treatment or condition of the patient, e.g., the impact and quality of the chemotherapy treatment. | A data analytics module with a feature for predicting the upcoming treatment outcome (i.e., toxicity level and side effects expected from the different chemotherapy treatments like scheduled doses, cycles) using machine learning models.<br>The doctor can inspect predictions by inputting the treatment into a set of machine learning models. | With fabricated data we have developed a proof-of-concept predictor, with encouraging results.<br>However, re-training activity with real dataset is necessary for a real-life and more robust model with higher likelihood of generating accurate toxicity levels that can be used by the medical staff. | **Smart Patient Health Record:**<br>The SERUMS platform through the Data Lake integrates clinical notes and recommendations from different GPs/oncologists reviewing the case as long as the source database contains the required tagging established by SERUMS to operate the data retrieval.<br>**Privacy Preserving Machine Learning module:**<br>The SERUMS’ machine learning |

| No. | Challenge/Need | Solution | Remarks/Notes | Technical Implication |
|---|---|---|---|---|
| | | | | module allows analyses of the existing treatments and recommends alternatives based on existing and/or synthetic data considering patients privacy is preserved while building/training these models. |
| **2** | **In compliance with the GDPR and data protection** | | | |
| a | Patients have the right to give or withdraw their consent to specific professionals (oncologists, GPs, professionals) for their data access at any time, in a secure and transparent fashion. The resulting system needs to respect this need.<br>Data from hospitals databases and the data collected from devices, or the patient's home environment, need to be integrated considering patients' consent. | The system maintains *data privacy* by showing medical data only to authorised users based on personalised access rules. The system guarantees *ownership verification* as only reliable and verified sources will be included.<br>*Data integrity* is achieved by means of end-to-end encryption through all the transmission channels. *Transparent and traceable transactions* are registered in a ledger supported by a blockchain. | Patients are allowed to give or withdraw access under their *own personal reasons* and following *government laws and institutions policies*.<br>In principle, the *patient will be the owner of her data*, for that she will decide who has access to it, if it complies with the national and institutional regulations.<br>Different healthcare providers have varied sets of static information and dynamic information stored in their *own proprietary formats* in several databases. Personal monitoring devices from patients acquire medical information in different formats. | **Personalised User Authentication and Blockchain:**<br>The SERUMS platform through an integrated interface to define *access rules*, links the features of the *blockchain and data lake components* to retrieve requested data only for authenticated and authorised users. This interface enables the user to interact with formal definition of access rules through a more intuitive natural language version of such rules.<br>Patients can authorise access over well-defined data categories (called tags), thus providing high granularity for defining rules.<br>**Smart Patient Health Record:**<br>In both cases medical data (from hospitals and from out-of-hospitals environments) are integrated in the data lake with a tagging scheme.<br>**Blockchain:**<br>The blockchain module maintains a registry of each transaction that will ensure accountability through audit trails. |

**Table 3 System requirements for USTAN User Story**

# 3 Proof of Concept

The third Proof of Concept took place in March and April 2022 at the three end-user locations. In this section, we will elaborate on the PoC measurements and how these measurements were carried out.

In this consortium, three hospitals have been designated as end-users to carry out the PoC measurements and to test the future SERUMS policy. These three end-user locations are:

- Zuyderland Medical Centre (ZMC)
- Fundació Clínic per a la Recerca Biomèdica (FCRB)
- Edinburgh Cancer Centre (ECC)

Each end-user location developed a use case, as is described in Chapter 2. These use cases are used as the foundation for the PoC and the recruitment of participants.

## 3.1.1 Measurement design

The measurements were carried out both qualitatively, through semi-structured interviews and a focus group, and quantitatively, through usability metrics and questionnaires. For a comprehensive data collection, three stakeholder groups were included, which were patients, healthcare professionals, and IT staff.

Ethical approval was acquired for all three end user organisations as well as informed consent.

## 3.1.2 Patients

The initial focus in the collection of this stakeholder group was on finding patients that belong to the proposed hospital-specific use cases. For each patient, an online session of approximately 60 minutes was held. During the first half of the session, patients were guided through the user authentication system and the front-end of the SPHR, where they could control the sharing of the fabricated medical data. In the second half, the questionnaire was filled in. After the session, patients were requested to log in three more times to test password memorability. This was done on day 1, 3, and 6 after the initial session. The sessions with the patients at the end-user location were around the same time to minimise bias.

The questionnaires were prepared by UCY. The answers were used to gain information about Success Indicator 3 and could be divided into three broad sections:

i) information on perceived usability, perceived memorability, perceived security, and trust in the proposed Personalised User Authentication (PUA) system (KPIs 3.1 till 3.4).

ii) overall patient trust in the system (KPI 3.5).

iii) information on perceived usability, perceived data ownership, and perceived security in the Smart Patient Health Record (SPHR) system (KPIs 3.7 till 3.9).

Reaction- and progress time were measured when interacting with the authentication system, to substantiate Success Indicator 1. In addition, during these interviews, patients gave live feedback on the platform. Appendix 1 shows the participants' information letter that was given to (potential) interested patients. The interview guide and the questionnaire for the patients can both be found in Appendix 2 and 3.

## 3.1.3 Care professionals

Care professionals were carefully selected by the hospitals themselves and included in the PoC measurement after voluntary consent. The healthcare professionals that were included were specifically selected per hospital based on the proposed use case and included medical specialists as well as other healthcare providers (e.g., physiotherapists and nurses).

Data of the care professionals was collected using semi-structured interviews per end-user location, in which the questions corresponded to the questions from the questionnaire found in Appendix 4. These interviews took approximately 60 minutes. The questions were similar to those provided to the patients, however with a shift towards the perspective of the caregiver in relation to his patients instead of the sole perspective of the patient. This allowed the same KPIs being measured, except for KPI 3.5 since this KPI focuses on Patient Trust. (KPI 3.1 till KPI 3.4 and KPI 3.7 till KPI 3.9).

### 3.1.4 IT staff

The input from the IT staff participating in this PoC measurement was gathered through a focus group facilitated by the end-user locations and the technical partners. The IT staff's input mainly focused on the security of data processing, for the whole process and further developments of the SERUMS policy. Feedback from the security and IT experts is used for further refine the SERUMS technologies in the next development life cycle. For example, feedback on security aspects of the user authentication technology will be used as input and reported in D5.4 Report on Implementation and Verification of Final User Authentication System, Security Metrics and Authentication Policies and D7.7 Report on Technical Roadmap for SERUMS Technology.

The focus group with hospital IT staff can be viewed as a homogeneous internal focus group. Participants received an informative briefing upfront of the session to have a more in-depth discussion about the SERUMS Policy. Technical partners were present to facilitate these discussions. The focus groups lasted approximately one hour.

## 3.2 PoC execution

This section explains the PoC at the specific end-user locations.

### 3.2.1 PoC execution and Covid-19

PoC1 was physically executed at FCRB and ZMC. Due to COVID-19, PoC2 could not be executed physically and was executed digitally at FCRB, ZMC, and ECC. To minimise biases and to make sure that PoC3 could be compared to the first two PoCs it was carefully considered what method of execution would be used for PoC3. The trade-offs could be seen in Table 4. We considered: i) the possibility to compare the different PoCs, ii) prevention of biases and iii) the number of participants necessary. In addition, both Spain and The Netherlands were in lockdown in January 2022, therefore, it was decided to execute PoC3 completely digitally.

| Trade Offs | A physical PoC | Combination | A digital PoC |
|---|---|---|---|
| **Compared to other PoCs** | Physical PoC3 cannot be compared to PoC2. | | Cannot be compared to PoC1 (most components were not available then, so a comparison is less valuable). |
| **Information bias** | • Easier to assist when participants need help, this might affect the results.<br>• It is expected physical drawing patterns is easier (and more intuitive) compared to digital. | | • Difficult to assist when something is going wrong.<br>• It is expected that digital drawing patterns is less easy (and less intuitive) compared to physical drawing. |

| Trade Offs | A physical PoC | Combination | A digital PoC |
|---|---|---|---|
| **Selection bias** | The selection of participants differs per end-user location (easier for ZMC, less easy for ECC). | Use of both methods, raises the need for more participants. | The selection of participants differs per end-user location (easier for ECC, less easy for ZMC). |

**Table 4 Trade-offs for the execution of PoC3**

## 3.2.2 PoC3 execution at end-user locations

At ZMC the PoC took place between March 7th and April 7th, 2022. In four weeks, interviews with medical personnel, patients and a focus group with IT personnel were executed. Recruitment of the patients was done via the Zuyderland Panel representing the older population and the Zuyderland Client Board. If patients were open to participate in the research, informed consent was asked by the SERUMS project leader, and an appointment for the PoC participation was scheduled. Participants received a €50, - gift card, regardless of whether they finished successfully. In addition, some patients were recruited by word of mouth or via the use-case-related physician. In total, ZMC was able to include 31 patients, but unfortunately, the results of two participants were not useable and therefore not included in the research, resulting in 29 patients. In addition, four people, part of the medical staff, were interviewed. The last component of the PoC at ZMC was the focus group conducted with three IT professionals.

At FCRB, the PoC took place between March 8th and April 1st, 2022. FCRBs patients were recruited via the use case-related department (endocrinology), where the doctor asked patients if they wanted to participate in the research. No rewards were offered to the participants. The focus groups and interviews with medical personnel took place in the last week of the PoC. No focus group with IT professionals was held. In total, FCRB was able to include 21 patients, of which eight were already included in earlier PoCs, and two physicians in PoC3.

At ECC, the PoC took place between March 23rd and April 1st. PoC3 was conducted by the USTAN team members, after approval from the University of St. Andrews, School of Computer Science Ethics committee. The activities to attract user participation included the distribution of a public information flyer that was developed for PoC2, to describe the SERUMS project in an accessible fashion, including a QR-code for interested participants to access further information from the project website. Volunteers were recruited via social media (for example, in Facebook groups) to ensure mostly local patients were interviewed. The recruitment announcement was shared in local Facebook groups across Fife, Tayside, and Edinburgh. Potential participants were asked to express their interest in the SERUMS project by email to the SERUMS email address.

Interviews were executed via Microsoft Teams or Zoom with at least two members of the USTAN team. After answering both the evaluation questionnaire and the three post-study emails, participants received a £10 Amazon Voucher in retribution for their time and broadband usage testing the SHCS. In total, they were able to include 32 patients in the research, of which one (1) is a healthcare professional and three (3) are IT personnel.

Table 5 shows the number of participants that were included at all end-user locations.

| | ZMC | FCRB | ECC | Proposed |
|---|---|---|---|---|
| **Patients** | 29 | 21 | 28 | 25 |
| **Medical personnel** | 4 | 2 | 1 | 5 |
| **IT staff** | 3 | - | 3 | 5 |

**Table 5 Number of participants included in PoC3**

# 3.3 Remarks on the evaluation method

After gathering data during the PoCs, the data needs to be transformed into KPIs. The chosen method for calculating the KPIs is the AMPI Index [1] (De Muro et al., 2011), shown in equation 1. This method is chosen, because of the different units and ranges of the KPIs. Table 6 shows the minimum and maximum values for each KPI. In the following paragraphs, the weighted coefficient and success metrics, shown in Table 6, are elaborated.

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

*Equation 1. AMPI index formula*

## 3.3.1 KPI and metric weights

After PoC1 it was found out that there were differences in the importance of the different measurements (KPIs and metrics) and that reporting them with the same importance into the Success Indicators would indicate a misinterpretation of the impact of the Success Indicators. To solve this problem, the technical partners evaluated the KPIs and agreed on a list of coefficients that would be used to weigh all metrics/KPIs.

These weights, as shown in Table 6, can be in the range from 0 to 3:

0: This metric should not affect the Success Indicator.
1: This measurement does not affect the Success Indicator in a noticeable manner.
2: This measurement does affect the Success Indicator in an important way.
3: This measurement does have great importance in the Success Indicator.

In some cases, the coefficient was set up depending on the ability of the partners to obtain a trusted value for the metric. This is the case in the metrics Theoretical Entropy for graphical and textual passwords as the practical entropy is a more representative metric for measuring password security strength [3].

During PoC3 we were able to implement the Enhanced Privacy Models and Predictive Data Analytics Models into the SERUMS system. This means that we were able to measure and explain KPIs 2.3: Enhanced Model Privacy, 3.6: Model Utility and Privacy and 4.1: Model Utility Accuracy. Unfortunately, due to the delayed integration of the Predictive Data Analytics Models, caregivers were not able to experience and test these models. Therefore, we are unable to report an outcome value for KPI 3.6.

Additional explanation and justification on these coefficients can be found in our previous Deliverable 7.3 and 7.5 in chapter 4.1.2.

| SI | KPI | Measurement | Coefficient | Minimum value | Maximum value | Success Metric |
|---|---|---|---|---|---|---|
| 1 | KPI 1.1: Guessability | Theoretical Entropy Graphical | 0 | 1 bit | 30.1 bits | N/A |
| | | Theoretical Entropy Textual | 0 | 1 bit | 105.4 bits | N/A |
| | | Practical Entropy Graphical | 3 | 1 bit | 35 bits | 24 bits |
| | | Practical Entropy Textual | 1 | 1 bit | 104.87 bits | 30 bits |
| | | Guess Number Graphical | 3 | 1 bit | 30.1 bits | N/A |
| | | Guess Number Textual | 1 | 1 bit | 104.87 bits | N/A |
| | | Textual password complexity | 1 | 0% | 100% | >70% |
| | | Graphical password complexity | 3 | 0% | 100% | >70% |
| | | Push notification accuracy | 1 | 0% | 100% | >80% |
| | KPI 1.2: Password leaks (through social engineering) | Memory time | 2 | 0 | 168 hours | 96 |
| | | Human guessing attack | 1 | 1 | 1.16E+9 | N/A |
| | KPI 1.3: System vulnerability | | 2 | 24 | 240 | +10% from baseline |
| 2 | KPI 2.1: Password cracking resistance | | 2 | 0% | 100% | >51.8% |
| | KPI 2.2: Data Breaches | | 3 | 10 | 110 | +10% from baseline |
| | KPI 2.3: Enhanced model privacy | | 1 | 10x decrease | 0.1x decrease | < 1x decrease |
| | KPI 2.4: Granular access to patient record | | 2 | 1 | 4 | 4 |
| | KPI 2.5: Authorization data integrity | | 1 | 1 | 4 | 4 |
| | KPI 2.6: Efficiency of cross-country patient data sharing | | 1 | 1 | 4 | 4 |
| 3 | KPI 3.1: Perceived usability | | 2 | 0% | 100% | >70% |
| | KPI 3.2: Perceived memorability | | 1 | 1 | 5 | >3.8 (>70%) |
| | KPI 3.3: Perceived security | | 2 | 1 | 5 | >3.8 (>70%) |
| | KPI 3.4: Trust in the proposed PUA scheme | | 3 | 1 | 5 | >3.8 (>70%) |
| | KPI 3.5: Patient Trust | | 2 | 1 | 5 | >3.0 (>50%) |
| | KPI 3.6: Data Analytics Model Utility | | 0 | No results available | | |
| | KPI 3.7: Perceived Usability of SERUMS System | | 2 | 1 | 5 | >3.8 (>70%) |
| | KPI 3.8: Perceived Data Ownership in the SERUMS System | | 3 | 1 | 5 | >3.8 (>70%) |
| | KPI 3.9: Perceived Security in the SERUMS System | | 3 | 1 | 5 | >3.8 (>70%) |
| 4 | KPI 4.1: Data Analytics Model Utility | | 1 | 0.1x increase | 10x increase | > 1x increase |

**Table 6 All metrics used to calculate the Success Indicators**

### 3.3.2 Success Metrics

To define a Success Indicator as a success, each Success Indicator contains (in brackets) a benchmark value that should be achieved by the end of the project. After PoC2, it was observed that the originally proposed benchmarks for the Success Indicator were defined as an increase of a certain factor compared to the baseline, e.g., an increase of factor two. Because this was not compatible with the AMPI method and several KPIs could not be compared to a baseline, a different benchmark was needed. Therefore, the technical partners evaluated the KPIs and assigned each one a success metric. Using these KPI success metrics, we were able to create a benchmark for the Success Indicators using the same AMPI method and weighted coefficients.

It is important to mention that there are no success metrics for the Theoretical Entropy and Guess Numbers in KPI 1.1, and the Human Guessing Attack in KPI 1.2. The reason is that there was insufficient literature available to define these, and the baseline for these metrics could not be measured during the project due to security and privacy issues with patient data. To resolve this issue, these success metrics were not considered when defining the overall benchmark for the Success Indicators.

## 3.4 Planning

In total three PoC measurements were carried out throughout the SERUMS consortium. The first PoC, which is described in D7.3, was carried out in Month 13 of the project (January and early February 2020). The second PoC, which is described in D7.5, was carried out in Month 24 of the project (December 2020). The third and final PoC measurement was performed at all three end-user locations in Months 39 and 40 (March and April 2022).

After the first two PoCs (M13 & M24) the results per end-user were evaluated and the lessons learned were identified to improve the design of the system and the execution of PoC3, including the questionnaires and interview guides developed by UCY. Besides, the results of the different end-users have been compared and evaluated for further improvements in the period M25 till M40. The results of the last PoC (M40) will be compared with the results obtained earlier in the process, to draw a conclusion about the improvement of the system. In addition, the outcomes will be used to define possible improvements that can be part of the technical roadmap (D7.7).

Between Proof of Concepts, stakeholders were informed of the progress of the project through several newsletters. The results of the PoC will be shared with the stakeholders as part of the press release upon the closing of the SERUMS Project.

# 4 Evaluation of the Third Proof of Concept

Through executing the PoC, we gathered results using interviews and questionnaires that jointly were used to measure the metrics defined for each Key Performance Indicator (KPI) mentioned in the Deliverable 7.5. These KPIs allowed the end-users to report the values of the evaluation of the Final Version of the SERUMS technologies.

Although the amount of KPIs during the evaluation of the third PoC was similar to the second PoC, the content of some KPIs has changed. Specifically, this PoC, for the first time, shows results from the integrated privacy models in KPI 2.3 and data analytics models in KPIs 3.5 and 4.1. Moreover, several KPIs now accounted for international data-sharing. This is most apparent in the extended questionnaire for KPIs 3.7 to 3.9.

As defined in the Deliverables 7.4 and 7.5, four types of Success Indicators, that pertain to the next impacts, will be reported in the following pages

1. Quantifiable improvement in the secure provision of health and care services
2. Significantly reduced risk of data privacy breaches
3. Increased patient trust in the provision of smart health care
4. Increased patient safety

## 4.1 Evaluation of impact

The SERUMS project has identified three impacts that guided the development of the SERUMS Technologies, namely:

- Impact I = Quantifiable improvement in the secure provision of health and care services
- Impact II = Significantly reduced risk of data privacy breaches
- Impact III = Increased patient trust and safety

To specify the improvements necessary to reach these Impacts, the SERUMS project defined four Success Indicators. As explained before in 3.3.2., after PoC2 these Success Indicators were redefined and used to evaluate the Impact. The redefined Success Indicators for each Impact can be found in the explanation below.

For Impact I, the Success Indicator is defined as:

- S1) Quantifiable improvement in secure provision of health and care services (AMPI score of at least 64%), 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.

For Impact II, the Success Indicator is defined as:

- S2) Significantly reduced risk of data privacy breaches (AMPI score of at least 65%), evidenced by quantitative metrics showing the quantity of private data that is revealed through several common cyber-attacks.

Impact III has two Success Indicators attached to it. These are:

- S3) Quantifiable improvement in levels of patient trust in the provision of smart health care (AMPI score of at least 68%), evidenced by patient surveys and questionnaires.
- S4) Quantifiable improvement in patient safety (AMPI score of at least 50%), 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.

Table 7 shows the results of each SI during the PoCs in relation to the benchmark. In this last PoC all Success Indicators were measured. Going into more detail, the benchmark for S1 was already reached during PoC2 and was improved on during PoC3. For S2 we have achieved a significant increase compared to the baseline and were able to reach the benchmark. The patient trust in SERUMS, measured by S3 increased compared to PoC2 and the baseline, exceeding the assigned benchmark. Finally, the data analytics models tested in S4 showed a desired increase in model accuracy and privacy. It is important to note that the outcome of PoC2 might have changed between D7.5 and this deliverable (D7.6), due to a small correction in the minimum or maximum values of the KPIs, or because new insights revealed a miscalculation.

| Impact | Success Indicator | Benchmark | Baseline | PoC1 | PoC2 | PoC3 |
|---|---|---|---|---|---|---|
| **Impact I** | **S1** | 64 | 45 | N/A | 66 | 68 |
| **Impact II** | **S2** | 70 | 38 | N/A | 63 | 80 |
| **Impact III** | **S3** | 68 | 70 | 74 | 74 | 77 |
| | **S4** | 50 | N/A | N/A | N/A | 66 |

**Table 7 Success Indicator values for Baseline, Benchmark, and the PoCs**

### 4.1.1 Success Indicator 1

The Success Indicator that is used for measuring SERUMS progress and specific impact in terms of "Secure provision of health and care services" (Impact I), is:

- **S1)** Quantifiable improvement in secure provision of health and care services (AMPI score of at least 64%), 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, we provide the definition of the KPIs used to define the outcome of S1, as well as their respective results for the third Proof of Concept (PoC3). The following SERUMS Technologies have contributed to achieving S1, namely:

- Personalised User Authentication (PUA)
- Smart Patient Record (SPR)
- Verification Technologies (VOT)

| Success Indicator | KPI | Technology | Benchmark | PoC3 |
|---|---|---|---|---|
| **S1** | 1.1: Guessability | PUA | 61 | 75 |
| | 1.2: Password Leaks (through social engineering) | PUA | 71 | 86 |
| | 1.3: System Vulnerability | SPR | 63 | 52 |
| | **Outcome** | | **64** | **68** |

**Table 8. Shortened table for S1**

#### 4.1.1.1 KPI 1.1 Guessability

Below the guessability is shown. It consists of theoretical and practical entropy, guess number, password complexity and push notification accuracy, for both groups of patients (one with personalised pictures and one with generic pictures.

| KPI | Picture | | Passphrase |
|---|---|---|---|
| | Personalised | Generic | |
| **Theoretical entropy** | 30.10 bits | 30.10 bits | 104.87 bits |
| **Practical entropy** | 25.57 bits | 23.53 bits | 46.25 |
| **Guess number** | 49965672 | 12148995 | 8.3683E+13 |
| **Password complexity** | 76.40% | 67.55% | 79.08% |
| **Push notification accuracy** | 100% | | 100% |

**Table 9 KPI 1.1 Guessability**

### 4.1.1.1.1 Theoretical Entropy

Entropy is a measure on how difficult it is to guess a password. Entropy is measured as the expected value (in bits) of the information contained in a string and can be related to authentication key strength by providing a lower bound on the expected number of guesses to find a text. 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:

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

Table 10 summarises the theoretical entropy for picture and textual passwords across organisations. Given that we report theoretical entropy, according to the policy applied at each organisation, the metric scores can be theoretically the same as the maximum value. Also, passphrases have significantly higher values compared to graphical passwords given that the textual password policy allows a high number of characters (minimum length of 16 characters) to be used.

| | | ZMC | FCRB | USTAN | TOTAL |
|---|---|---|---|---|---|
| **Picture** | **Score** | 30.1 bits | 30.1 bits | 30.1 bits | 30.1 bits |
| | **AMPI** | 100 | 100 | 100 | 100 |
| **Passphrase** | **Score** | 105.4 bits | 105.4 bits | 105.4 bits | 105.4 bits |
| | **AMPI** | 100 | 100 | 100 | 100 |

**Table 10 KPI 1.1 Guessability – Theoretical Entropy**

### 4.1.1.1.2 Practical Entropy

A true measure of theoretical entropy cannot be computed in cases of user-chosen authentication keys since users tend to choose more memorable than random keys. For measuring practical entropy, we have considered the work and results described in [2-5] which provide estimates of practical entropy of different password policies.

With regards to passphrase, the benchmark is based on state-of-the-art estimates indicating that the practical entropy of 16-character passwords is 44.67 bits [3].

With regards to picture passwords, the benchmark is based on related work indicating that the theoretical entropy of picture password created on generic images is 21.96 bits (*$log_2$*(4090000) = 21.96) [8].

| | | ZMC | FCRB | USTAN | TOTAL |
|---|---|---|---|---|---|
| **Picture** | **Score** | 25.62 bits | 25.44 bits | 25.61 bits | 25.55 bits |
| | **AMPI** | 72 | 72 | 72 | 72 |
| **Passphrase** | **Score** | 46.93 bits | 45.57 bits | 46.27 bits | 46.25 bits |
| | **AMPI** | 45 | 43 | 44 | 44 |

**Table 11 KPI 1.1 Guessability – Practical Entropy**

| | ZMC | FCRB | USTAN | TOTAL |
|---|---|---|---|---|
| **Personalised** | 25.62 bits | 25.44 bits | 25.61 bits | 25.55 bits |
| **Generic** | 23.70 bits | 23.53 bits23.40 bits | 23.40 bits | 23.54 bits |

**Table 12 Practical entropy across image types (personalised vs. generic images) per end-user organisation**

Results indicate that the practical entropy of passphrases created in the PoC3 authentication system is higher in all three end-user organisations compared to the practical entropy estimates from the literature [3]. Similarly, the practical entropy of picture passwords created in the PoC3 authentication system is higher in all three end-user organisations compared to the practical entropy of the related work [8]. Furthermore, the practical entropy of the picture passwords created on personalised images in the PoC3 authentication system is higher than the practical entropy of the picture passwords created on generic images across all three end-user organisations.

#### 4.1.1.1.3 Guess Number

Guess number refers to how many guesses a particular password-cracking algorithm with training data would take to guess a password.

Table 13 summarises the guess number for picture and textual passwords, and Table 14 further summarised the guess number for personalised vs. generic graphical passwords across organisations. Accordingly, for graphical passwords, all organisations scored a higher guessability based on the defined success metric (24 bits). Similarly, for textual passwords all organisations scored a higher guessability based on the defined success metric (30 bits).

| | | ZMC | FCRB | USTAN | TOTAL |
|---|---|---|---|---|---|
| **Picture** | **Score** | 25.63 bits | 25.44 bits | 25.61 bits | 25.56 bits |
| | **AMPI** | 85 | 84 | 85 | 85 |
| **Passphrase** | **Score** | 46.93 bits | 45.57 bits | 46.27 bits | 46.26 bits |
| | **AMPI** | 44 | 43 | 44 | 44 |

**Table 13 KPI 1.1 Guessability – Guess Number**

| | ZMC | FCRB | USTAN | TOTAL |
|---|---|---|---|---|
| **Personalised** | 25.62 bits | 23.70 bits | 25.44 bits | 23.54 bits |
| **Generic** | 25.61 bits | 23.40 bits | 25.56 bits | 23.55 bits |

**Table 14 KPI 1.1 Practical guess number across image types (personalised vs. generic images) per end-user organisation**

Results indicate that the number of guesses required to crack the picture passwords created on personalised images in the PoC3 authentication system is higher than the number of guesses required to crack the picture passwords created on generic images across all three end-user organisations.

### 4.1.1.1.4 Password Complexity

For measuring textual password complexity, we have implemented Dropbox's *zxcvbn*, which is a widely applied and realistic password strength estimator. The minimum and maximum value of textual password complexity is 0% and 100% respectively. The higher the score, the more complex the password is. Textual password complexity is not applicable for the baseline study since this information was not available by the organisations.

An additional measure for graphical passwords is graphical password complexity, which describes how complex a graphical password is based on the users' image selections and gestures. For measuring graphical password complexity, we used a heuristic approach by considering state-of-the-art knowledge on picture gesture authentication [4, 5, 6]. Taking into consideration that the tap (click) is the least complex gesture, while the line is the more complex gesture [4], we set our initial complexity heuristic as follows:

*Combination of gestures* → *Complexity*

- 3 taps → 40%
- 3 circles → 80%
- 3 lines → 100%

*# Disregarding order*

- 1 tap & 2 circles → 50%
- 2 taps & 1 circle → 50%
- 1 tap & 1 line & 1 circle →70%
- 2 taps & 1 line → 70%
- 1 tap & 2 lines →70%
- 2 circles & 1 line →70%
- 2 lines & 1 circle →80%

As the proximity of different gestures impacts the overall complexity of the password (*e.g.*, different gestures on the same *x*, *y* segment on the grid are less secure), we take an extra step to either penalise (-20%) password combinations that include gestures that are in close proximity (as defined by the threshold of a circle of 3 segments radius [4]), or reward (+20%) password combinations that do not include gestures in close proximity. Graphical password complexity is not applicable for the baseline study since all three end-user organisations did not implement a graphical password system.

With regards to passphrase, the benchmark is based on Dropbox's zxcvbn password strength estimator, which returns a password strength estimation as a score in the range between 0 and 47. Accordingly, the middle value

[7] https://github.com/dropbox/zxcvbn

of this scoring scheme, i.e., score = 2 (which can be considered as 60%) was considered as a baseline and indicates a somewhat guessable password.

With regards to picture passwords, the benchmark is based on related work indicating that the gesture tap is more common than lines or circles [5]. Accordingly, based on the heuristic approach described above, we consider as baseline a combination of three taps (i.e., 40%) that does not include gestures in proximity (i.e., +20%), resulting in a complexity of 60%.

| | | ZMC | FCRB | USTAN | TOTAL |
|---|---|---|---|---|---|
| **Picture** | **Score** | 74.61% | 77.78% | 76.31% | 76.23% |
| | **AMPI** | 75 | 78 | 76 | 76 |
| **Passphrase** | **Score** | 80.00% | 80.00% | 77.64% | 79.21% |
| | **AMPI** | 80 | 80 | 78 | 79 |

**Table 15 KPI 1.1 Guessability – Password Complexity**

| | ZMC | FCRB | USTAN | TOTAL |
|---|---|---|---|---|
| **Personalised** | 77.78% | 74.61% | 76.31% | 76.23% |
| **Generic** | 68.57% | 66.36% | 67.50% | 67.48% |

**Table 16 Password complexity across image types (personalised vs. generic images) per end-user organisation**

Results indicate that the complexity of the passphrases created in the Poc3 authentication system is higher than the benchmark in all three end-users organisations. Similarly, the complexity of the picture passwords created in the Poc3 authentication system is higher than the benchmark in all three end-users organisations. Furthermore, we note that individuals who created picture passwords using personalised images created more complex passwords compared to individuals who created picture passwords using generic images across all three end-users organisations.

### 4.1.1.1.5 Push Notification Accuracy

In the third evaluation study, we deployed and evaluated the two-factor authentication system (2FA) that was implemented as a mobile application (SERUMS Authenticator) and optionally installed by the participants on their smartphones. The effectiveness of the 2FA system is measured through push notification accuracy, which measures the accuracy of the users' approval of push notifications.

The table below summarises the number of users that enabled the 2FA option and installed the SERUMS Authenticator app and whether they successfully authenticated or not using the mobile application. We note that push notification accuracy scored a 100% success rate in all three end-users organisations.

| ZMC | | FCRB | | USTAN | |
|---|---|---|---|---|---|
| **# of users** | **Success rate** | **# of users** | **Success rate** | **# of users** | **Success rate** |
| 21 | 100% | 18 | 100% | 27 | 100% |

**Table 17 KPI 1.1 Guessability – Push Notification Accuracy**

### 4.1.1.2 KPI 1.2 Password Leaks (through Social Engineering)

#### 4.1.1.2.1 Memory Time

Memory time was measured over time by considering actual login attempts of the end-users. Memory time refers to the greatest length of time between a password creation and a successful password login using the same password. Large memory times indicate higher memorability. Memorable passwords lead to potentially less social engineering-based password leaks as users do not need to follow coping strategies (*e.g.*, write down their passwords).

Memory time data could not be measured for the baseline study since the relevant data was not supported by the existing authentication systems at the end-user organisations (or not available due to privacy regulations and policies of the corresponding organisation). In addition, given that memory time requires participants using the system over time, we did not measure this in PoC1 since the aim of the first evaluation of the user authentication system was to elicit the users' perceptions and likeability towards the first PoC authentication system.

Another metric for memorability relates to the time needed to login. For the baseline authentication system, we received summarised password reset data from ZMC. The table below summarises the number of resets and the average amount of days between the resets at ZMC starting from January 01, 2019, until October 31, 2019.

The user study on the memorability aspects of the PoC3 authentication system took one week. Hence, the maximum memory time that someone could achieve was approximately 168 hours (7 days * 24 hours). Accordingly, we consider as baseline the middle value of the overall duration of the study (i.e., 168/2=84 hours), which indicates a considerable memorable password.

With regards to the memory time for the passphrase authentication type, which was optional to setup, we note that the total number of users who used this authentication type to login was as follows: i) In the case of ZMC, there were 16 out of 36 participants; ii) In the case of FCRB, there were 3 out of 23 participants; and iii) In the case of USTAN, there were 10 out of 32 participants.

| | | ZMC | FCRB | USTAN | TOTAL |
|---|---|---|---|---|---|
| **Picture** | **Score** | 156 | 134.4 | 137.14 | 142.51 |
| | **AMPI** | 93 | 80 | 81 | 85 |
| **Passphrase** | **Score** | 121.5 | 120 | 132 | 124.5 |
| | **AMPI** | 72 | 72 | 79 | 74 |

**Table 18 KPI 1.2 Memory time (in hours) – maximum 168 hours (7 days * 24 hours)**

| | ZMC | FCRB | USTAN | TOTAL |
|---|---|---|---|---|
| **Personalised** | 156.0 | 134.4 | 137.1 | 142.5 |
| **Generic** | 124.4 | 115.2 | 136.0 | 125.2 |

**Table 19 KPI 1.2 Memory time (in hours) across image types (personalised vs. generic images) per end-user organisation**

|  | ZMC | FCRB | USTAN | TOTAL |
|---|---|---|---|---|
| **Picture** | 8.04 | 5.07 | 5.33 | 6.14 |
| **Passphrase** | 16.10 | 13.70 | 13.93 | 14.57 |

**Table 20 KPI 1.2 Login time (in seconds)**

|  | ZMC | FCRB | USTAN | TOTAL |
|---|---|---|---|---|
| **Personalised** | 8.04 | 5.07 | 5.33 | 6.14 |
| **Generic** | 12.61 | 5.34 | 9.82 | 9.25 |

**Table 21 KPI 1.2 Login time (in seconds) across image types (personalised vs. generic images) per end-user organisation**

Results indicate that the memory time of both the passphrase and picture password authentication types is higher than the benchmark in all three end-user organisations. In addition, we note that the memory time of picture passwords is higher compared to the memory time of passphrase. Furthermore, we note that individuals who created picture passwords using personalised images exhibit higher memory time compared to individuals using generic images across all three end-user organisations. With regards to login time, results indicate that individuals required more time to login using the passphrase authentication type compared to the picture password option. Moreover, we note that individuals who created picture passwords using personalised images exhibit lower login times compared to individuals using generic images across all three end-user organisations

#### 4.1.1.2.2 Human Guessing Attack

Given that when using the suggested personalised and retrospective approach the graphical password selections are based on the users' existing sociocultural experiences, it is probable that the individuals who share common experiences with the end-users might be able to guess their selections. To shed light on this aspect, a human attack study focusing on guessing vulnerabilities of the approach among people sharing common sociocultural experiences was conducted. Each session of the study embraced pairs of participants that were closely related (e.g., patients, medical staff, nurses, etc.) and who shared common experiences. In each session, we asked both participants to first create a graphical password, and then each participant was asked to guess the password selections of the other participant. A total of 62 individuals participated in the study, ranging in age between 28-60 years old.

To investigate how far the attackers' guessing selections were from the end-users' actual secret selections, we calculated the Euclidean distance between the 3 x, y segments provided by the attacker and the 3 x, y segments of the legitimate end-user. The figure below depicts the Euclidean distance of each gesture of each participant by disregarding the type and the exact order of the attackers' gestures and the end-user's gestures. Accordingly, among 186 gestures (3 gestures x 62 participants), 36 gestures (19%) were in proximity with the attacker's guessed selections.

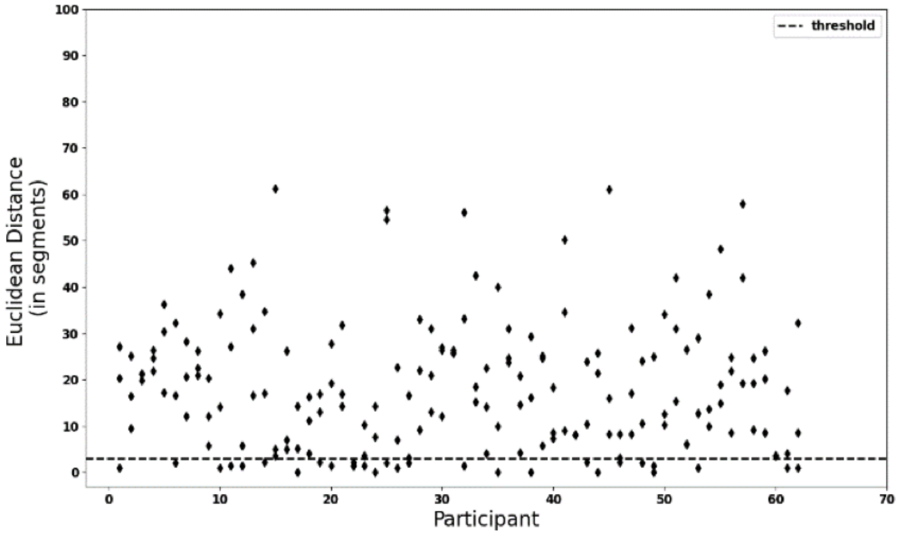


**Figure 3. Euclidean distance**

Furthermore, we compared the 3 attempts of each attacker with the legitimate end-user's stored password from the same pair of participants, simulating in principle an online guessing attack. From a total of 186 attacking guesses (3 attempts of each attacker x 62 participants), there was no successful attempt, yielding an online success guessing rate of 0%.

## 4.1.1.3 KPI 1.3 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 was used was both external network and internal network penetration testing. This allowed us to see how vulnerable the system is from the outside as well as once they have gained some form of access. Additionally, the security of the programming languages used was scored, as well as the lifespan of security support that is left.

The benchmark took the form of a survey which was handed to use case partners. The 19 questions corresponded to the security infrastructure in place to secure patient data. Due to the sensitive nature of the data, not all use case partners were able to provide data for all questions. Industry Knowledge was used to score these KPIs from 1-10 by looking for known vulnerabilities within the sector.

| | ZMC | FCRB | USTAN | SERUMS |
|---|---|---|---|---|
| **PoC3 score** | 183 | 109 | N/A | 131 |
| **PoC3 AMPI** | 0.67 | 0.44 | N/A | 0.56 |

**Table 22 KPI 1.3 System Vulnerability**

In this context, FCRB had increased system vulnerability compared to ZMC. Utilising more up to date security practices and programming languages resulted in a higher score for these systems. For SERUMS, automated suspicious activity flagging, regular access log monitoring, security matrix checking would have increased the security score even higher and exceeded those of ZMC, FCRB.

## 4.1.2 Success Indicator 2

The Success Indicator used for measuring SERUMS progress and specific impact in terms of "Significantly reduced risk of data privacy breaches" (IMPACT II), is:

- **S2)** Significantly reduced risk of data privacy breaches (AMPI score of at least 78%), evidenced by quantitative metrics showing the quantity of private data that is revealed through several common cyber-attacks.

Below, the definition is given of the KPIs that are used to define the outcome of S2, as well as their respective results for the third Proof of Concept (PoC3). The following SERUMS Technologies have contributed to achieving S2, namely:

- Credential Hardening (CH)
- Smart Patient Record (SPR)
- Privacy-preserving Data Analytics (PDA)
- Distributed Ledger Technology (DLT)
- Verification Technologies (VOT)

| Success Indicator | KPI | Technology | Benchmark | PoC3 |
|---|---|---|---|---|
| **S2** | **2.1: Password Cracking Resistance** | CH | 51.8 | 100 |
| | **2.2: Data Breaches** | SPR | 38 | 41 |
| | **2.3: Enhanced Model Privacy** | PDA | 50 | 66 |
| | **2.4: Granular Access to Patient Record** | DLT | 100 | 100 |
| | **2.5: Authorisation Data Integrity** | DLT | 100 | 100 |
| | **2.6: Efficiency of Cross-Country Patient Data Sharing** | DLT | 100 | 100 |
| | **Outcome** | | **70** | **80** |

**Table 23 Shortened version for S2**

### 4.1.2.1 KPI 2.1 Password Cracking Resistance

Password cracking rate is measured in a leaked database storing hardened credentials through an offline brute-force attack. Typically, this threat model assumes that the passwords are hashed using a cryptographic hash function and that the attacker can recompute the hashed passwords by trying combinations of known dictionary words. Core properties in the password cracking rate are: (a) the cryptographic hash function used, which depending on the computation overhead may reduce the rate of cracking attempts, and (b) the distribution of the passwords. Notice that, in SERUMS, the credential hardening offered by the system does not allow an attacker to crack any password, since recomputing the hash requires access to the TLS private key. In other words, an attacker that has no access to the TLS private key cannot compute any hash value (or (a), above, takes infinite time).

Now, assuming that the TLS private key of the system is stolen, then cracking is possible (that is, (a), above, takes finite time) and the rate of trials is depicted below. Numbers are presented with comparison to other popular hashing schemes. Cracking rate is the power you have to crack a password, which is proportional to how many hash computations you can do per second. Hence, we report cracking rate, which is measured to hash computations/sec.

Typically, such rates for normal password distributions (i.e., passwords that match the user preferences based on password leaks of English-based passwords we are aware so far) allow for a password cracking rate of around 51.80% as reported in the current literature (see Table 1 in https://eprint.iacr.org/2019/1188.pdf). Notice, that such cracking rate can be experienced by the SERUMS system only when the TLS private key is leaked. The baseline for this KPI is: “Baseline/state-of-the-art: 51.80% - based on a state-of-the-art paper published in an accredited computer security venue - IEEE Symposium on Security and Privacy (Oakland) - (see Table 1 in https://eprint.iacr.org/2019/1188.pdf)”

During PoC3 several technological and practical attempts were made to guess a password. We are happy to inform that all attempts were unsuccessful. Thus, meaning that SERUMS in uncrackable, assuming the TLS key is secure.

### 4.1.2.2 KPI 2.2 Data Breaches

KPI 2.2 includes the measurement of data that is able to be accessed by unauthorised or inappropriate sources. Using 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. Additionally, we can apply a score against the ease at which physical copies of the data can be generated.

This took form as a questionnaire that was given to the use case partners. Due to the sensitive nature of the questions, not all partners responded. Each result of the questionnaire was scored on a scale of 1 - 10, with 1 being critical and 10 being no known issues. The minimum score was 12 and the maximum score was 120 for 12 questions. The questions covered the access that staff have to patients’ records as well as the options available to create physical copies of the data. Not all questions were answered by the use case partners or were relevant in the case of SERUMS (such as removable media), so the AMPI value was used to compare the scores.

| | **ZMC** | **FCRB** | **USTAN** | **SERUMS** |
|---|---|---|---|---|
| **PoC3 score** | 65 | 49 | N/A | 47 |
| **PoC3 AMPI** | 0.54 | 0.44 | N/A | 0.46 |

**Table 24 KPI 2.2 Data Breaches**

SERUMS has not undergone security matrix testing or implemented automated suspicious activity flagging, both of which would boost its scores substantially, resulting in a higher AMPI value compared to ZMC or FCRB. SERUMS currently has a higher score compared to the previous PoC implementation.

#### 4.1.2.3 KPI 2.3 Enhanced Model Privacy

Model Privacy measures the ability of a model to preserve the privacy of the data used to train the model when releasing the model's output. Since there is always a trade-off between a model's privacy and a model's utility, the level of accuracy needs to be defined, in this case the percentage of correct predictions, at the privacy level was measured to be able to compare different approaches of privacy preservations.

To measure the level of privacy, the well-established mathematical framework of (e; δ)-differential privacy was used. Enhanced model privacy is the factor of increase in differential privacy when comparing two models at the same level of utility.

Since the actual level of privacy that a model can achieve is on the one hand dependent on the level of accuracy that needs to be achieved and on the other hand on the training dataset itself, no general statement can be made about the factor of model privacy enhancement of a privacy preserving model.

To evaluate privacy-preserving machine learning methods, a ratio, measuring the loss in accuracy because of decreasing privacy-loos bound for a fixed failure probability, is defined. The fabricated USTAN use case dataset was used to evaluate the developed methodology and compared with the state-of-the-art machine learning methods. The best performing existing machine learning method together with the optimised differentially private noise adding mechanism was considered as the reference method for a comparison.

It was observed that the developed methodology resulted on the fabricated USTAN use case dataset in a gain of accuracy by a factor of 2.1121 over the reference benchmark method. Due to the logarithmic nature of factorial increases, this resulted in an AMPI score of 66.

#### 4.1.2.4 KPI 2.4 Granular Access to Patient Record

This KPI measured how granular the solution offered the ability to manage the access to the patient record.

Four levels of permission granularity of patient record access with a scale of 1-4, where level 4 is the most satisfactory level, were defined. Since patients themselves can create/update/remove rules in the SERUMS interface, level 4 is reached. Using tags that are included in the access rules, access to the patients' record can be granted at a granular level by the patients themselves.

1. No digital access management of the patient record
2. Access can be managed by the organisation (e.g., hospital) at patient record level, which means the record can be accessed or not as a whole for the caregiver.
3. Access can be managed by the organisation (e.g., hospital) at a granular level (e.g., a subset of the patient record)
4. Access can be managed by the organisation (e.g., hospital) and the patients themselves at a granular level (e.g., a subset of the patient record)

| | ZMC | FCRB | USTAN | TOTAL |
|---|---|---|---|---|
| **PoC3 score** | 4 | 4 | 4 | 4 |
| **PoC3 AMPI** | 4 | 4 | 4 | 4 |

**Table 25 KPI 2.4 Granular Access to Patient Record**

#### 4.1.2.5 KPI 2.5 Authorisation Data Integrity

This KPI will be measuring how resilience the current system is handling the authorisation data.

In case a party on the DLT network is compromised, and it has been identified that data has been tampered with, the solution can identify the exact data that has been tampered with and retrieve the original value. We have defined 4 levels with a scale of 1-4 where level 4 is the most satisfactory level. The DLT solution aims to reach level 4.

1. No means to traceback when (authorization) data has been compromised.
2. Can retroactively track when data is compromised but cannot track which specific data was compromised.
3. Retroactive tracking when data is compromised and can identify which data has been compromised but cannot restore the original value.
4. Retroactive tracking when the data is compromised and can identify and restore the data that has been compromised.

| | ZMC | FCRB | USTAN | TOTAL |
|---|---|---|---|---|
| **PoC3 score** | 4 | 4 | 4 | 4 |
| **PoC3 AMPI** | 4 | 4 | 4 | 4 |

**Table 26 KPI 2.5 Authorisation Data Integrity**

Creation and updates of all access rules in the Blockchain were versioned including timestamps. If an access rule was compromised the earlier version of the rule was reinitiated. This cannot be done in an automated way via a user-interface. The Blockchain is not responsible to detect a compromised change of a rule if it receives a valid access token, as it relies on the token provided by the authentication module.

### 4.1.2.6 KPI 2.6 Efficiency of Cross-Country Patient Data Sharing

This KPI will be measuring the efficiency of cross-country patient data sharing. The 2 types of data sharing are out-bound; one has data to be shared to another hospital, and in-bound; patient data to be received from another hospital.

A scale of 1-4 for new KPI to measure how cross-country permissions for patient data sharing is managed**.**

1. Cross-country permission is managed manually
2. Only outbound is managed in an automated way
3. Both in-bound and out-bound are managed in an automated way
4. Patient is in control and can initiate the process in an automated way

Patients can create access rules via their SERUMS interface and assign cross-country organisations to them. The Blockchain module does not make a difference between out-bound and in-bound rules, they are handled the same when and organisation is assigned to a rule. After the user completes the creation in the interface, the rule will automatically become active in the SERUMS system and be granting access accordingly, no further manual intervention needed.

| | ZMC | FCRB | USTAN | TOTAL |
|---|---|---|---|---|
| **PoC3 score** | 4 | 4 | 4 | 4 |
| **PoC3 AMPI** | 4 | 4 | 4 | 4 |

**Table 27 KPI 2.6 Efficiency of Cross-Country Patient Data Sharing**

## 4.1.3 Success Indicator 3

As mentioned before, there are two Success Indicators that will be used for measuring SERUMS progress and specific impact in terms of "Increased patient trust and safety":

- S3) Quantifiable improvement in levels of patient trust in the provision of smart health care (AMPI score of at least 68%), evidenced by patient surveys and questionnaires.

- S4) Quantifiable improvement in patient safety (AMPI score of at least 50%), 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 definition is given of the KPIs that are used to define the outcomes of S3 and S4, as well as their respective results for the third Proof of Concept (PoC3). The following SERUMS Technologies have contributed to achieving S3 and S4, namely:

- Personalised User Authentication (PUA)
- Smart Patient Record (SPR)
- Privacy-preserving Data Analytics (PDA)
- Smart Health Centre System (SHCS)

| **Success Indicator** | **KPI** | **Technology** | **Benchmark** | **PoC3** |
|---|---|---|---|---|
| **S3** | **3.1: Perceived Usability** | PUA | 70 | 72 |
| | **3.2: Perceived Memorability** | PUA | 70 | 78 |
| | **3.3: Perceived Security** | PUA | 70 | 79 |
| | **3.4: Trust in the Proposed PUA Scheme** | PUA | 70 | 78 |
| | **3.5: Patient Trust** | SPR | 50 | 59 |
| | **3.6: Data Analytics Model Utility** | PDA | No results available | |
| | **3.7: Perceived Usability of SERUMS System** | SHCS | 70 | 85 |
| | **3.8: Perceived Data Ownership in the SERUMS System** | SHCS | 70 | 83 |
| | **3.9: Perceived Security in the SERUMS System** | SHCS | 70 | 77 |
| | **Outcome** | | **68** | **77** |
| **S4** | **4.1: Data Analytics Model Utility** | PDA | 50 | 66 |
| | **Outcome** | | **50** | **66** |

**Table 28 Shortened table of S3 and S4**

### 4.1.3.1 KPI 3.1 Perceived Usability

One of the aims of the PoC evaluations of the user authentication system was to get feedback from end-user patients on aspects such as likeability towards the suggested flexible and personalised approach in authentication, and the end-users' perceptions towards usability, memorability, security, and trust. For this purpose, a questionnaire by following state-of-the-art works and guidelines on usability, user experience, security, and trust (*e.g.*, SUS, AttrakDiff, Technology Acceptance models, etc.) was designed.

With regards to perceived usability, questions that relate to the password creation process and login, *e.g.*, *"Overall, how difficult, or easy do you find the password creation task?"*, *"Overall, how difficult, or easy do you find the login task?"*, *"I could easily log on to the FlexPass password system"*, etc. had been asked. Users rated the statements through a 5-point Likert scale (*e.g.*, 1: Not at all - 5: Absolutely).

Based on the literature, the average SUS score is 68% [9, 10]. In case the score is significantly under 68%, the system entails various usability issues that need improvement, while a score around and above 68%, indicates that the system entails good usability practices. We strive to reach at least 70% with the SERUMS System. Top scores for usability are considered 80%.

| | ZMC | FCRB | USTAN | TOTAL |
|---|---|---|---|---|
| **SUS score** | 67.84% | 76.32% | 70.58% | 70.81% |
| **SUS AMPI** | 68 | 76 | 71 | 71 |

**Table 29 KPI 3.1 Perceived Usability**

| Likeability | Extremely | Very much | Moderately | Slightly | Not at all |
|---|---|---|---|---|---|
| **USTAN** | 20 | 8 | 3 | 1 | 0 |
| **ZMC** | 14 | 12 | 2 | 1 | 0 |
| **FCRB** | 9 | 6 | 0 | 1 | 1 |
| **Total** | **43** | **26** | **5** | **3** | **1** |

**Table 30 KPI 3.1 Perceived Usability – User responses**

User responses on the System Usability Scale (SUS), where non-significantly lower in PoC3 compared to PoC2 for ZMC (PoC2: 74.58% vs. PoC3: 67.84%), FCRB (PoC2: 80% vs. PoC3: 76.32%) and USTAN (PoC2: 72.14 vs. PoC3: 70.58%), with an overall score 70.81% for PoC3 (vs. 74.77% in PoC2).

Overall, we conclude that the FlexPass system scores well in usability, given that it scored +70% in both PoC2 and PoC3, nevertheless, given that the score is below 80%, there are still aspects that require improvements.

Furthermore, when end-users were asked whether they like the personalised and flexible approach for user authentication, most users extremely (43/78) or very much (26/78) liked the idea, with five users moderately and three slightly liking the idea, while one user did not like the idea.

### 4.1.3.2 KPI 3.2 Perceived Memorability

Like perceived usability, participants were questioned on whether they effectively recalled their passwords and whether the login process was mentally demanding. Users rated the statements through a 5-point Likert scale (*e.g.*, 1: Not at all - 5: Absolutely). Scores of 3.5 (70%) and above indicated good levels of the measured variable.

| | ZMC | FCRB | USTAN | TOTAL |
|---|---|---|---|---|
| **PoC3 score** | 4.06 | 4.29 | 4.03 | 4.1 |
| **PoC3 AMPI** | 76 | 77 | 82 | 78 |

**Table 31 KPI 3. 2 Perceived Memorability**

| Memorability | No | Moderate | Strong |
|---|---|---|---|
| **ZMC** | 4 | 1 | 24 |
| **FCRB** | 1 | 2 | 14 |
| **USTAN** | 3 | 6 | 23 |
| **Total** | **8** | **9** | **61** |

**Table 32 KPI 3. 2 Perceived Memorability – User responses**

Overall, all users across organisations perceived the FlexPass system as memorable and they could effectively recall their password. Scores on perceived memorability did not significantly change in PoC3 compared to PoC2. Specifically, the score of perceived memorability in ZMC slightly dropped from 4.2 to 4.06, in FCRB from 4.45 to 4.29 and in USTAN from 4.09 to 4.03.

### 4.1.3.3 KPI 3.3 Perceived Security

Following state-of-the-art user studies in usable security research [11, 12], for perceived security, participants were questioned on whether they believe the user authentication system is secure, whether they believe their password is strong, etc. Example questions include *"Overall, how secure do you find the FlexPass password system?"*, *"How strong do you believe a FlexPass password is?"*, etc. Users rated the statements through a 5-point Likert scale (*e.g.*, 1: Very insecure - 5: Very secure). Scores of 3.5 (70%) and above indicated good levels of the measured variable.

|  | ZMC | FCRB | USTAN | TOTAL |
|---|---|---|---|---|
| **PoC3 score** | 4.06 | 4.23 | 4.15 | 4.14 |
| **PoC3 AMPI** | 77 | 81 | 79 | 79 |

**Table 33 KPI 3. 3 Perceived Security**

|  | Organisation | Not secure | Medium | Secure | Very Secure |
|---|---|---|---|---|---|
| **Security** | **ZMC** | 2 | 6 | 8 | 13 |
| **FCRB** | **FCRB** | 0 | 4 | 5 | 8 |
| **USTAN** | **USTAN** | 1 | 8 | 8 | 15 |
| **Total** | **Total** | **3** | **18** | **21** | **36** |
| **Password strength** | **ZMC** | 3 | 3 | 9 | 14 |
|  | **FCRB** | 1 | 1 | 8 | 7 |
|  | **USTAN** | 3 | 6 | 11 | 12 |
|  | **Total** | **7** | **10** | **28** | **33** |

**Table 34 KPI 3.3 Perceived Security - Specific results on perceived security and password strength**

Overall, all users across organisations perceived the FlexPass system as secure and their passwords were strong. Scores on perceived security did not significantly change in PoC3 compared to PoC2. Specifically, the score of perceived security in ZMC dropped from 4.41 to 4.06, in FCRB it dropped from 4.59 to 4.23 and in USTAN it increased from 3.85 to 4.15. Total score of perceived security in PoC3 is 4.14 (vs. 4.2 in PoC3)

### 4.1.3.4 KPI 3.4 Trust in the Proposed PUA Scheme

For perceived trust, participants were questioned about their trust towards the user authentication system technology, its ability to protect their data privacy, their trust on security and trust to keep their data safe from cybercriminals. Users rated the statements through a 5-point Likert scale (*e.g.*, 1: Not at all - 5: Absolutely). Scores of 3.5 (70%) and above indicated good levels of the measured variable.

| | **ZMC** | **FCRB** | **USTAN** | **TOTAL** |
|---|---|---|---|---|
| **PoC3 score** | 4.37 | 4.00 | 4.03 | 4.15 |
| **PoC3 AMPI** | 84 | 75 | 76 | 78 |

**Table 35 KPI 3.4 Trust in the Proposed PUA Scheme**

| | **Organisation** | **Low** | **Moderate** | **High** |
|---|---|---|---|---|
| **Trust in Technology** | **ZMC** | 1 | 1 | 27 |
| | **FCRB** | 1 | 2 | 14 |
| | **USTAN** | 0 | 6 | 26 |
| | **TOTAL** | **2** | **9** | **67** |
| **Trust in Privacy** | **ZMC** | 3 | 2 | 24 |
| | **FCRB** | 1 | 2 | 14 |
| | **USTAN** | 1 | 11 | 20 |
| | **TOTAL** | **5** | **15** | **58** |
| **Trust in Security** | **ZMC** | 4 | 4 | 21 |
| | **FCRB** | 1 | 2 | 14 |
| | **USTAN** | 6 | 8 | 18 |
| | **TOTAL** | **11** | **14** | **53** |
| **Trust in Cybersecurity** | **ZMC** | 2 | 2 | 25 |
| | **FCRB** | 1 | 4 | 12 |
| | **USTAN** | 1 | 9 | 22 |
| | **TOTAL** | **4** | **15** | **59** |

**Table 36 KPI 3.4 Trust in the Proposed PUA Scheme – User responses**

Overall, FlexPass scored high in perceived trust with the majority of users scoring high levels of trust towards the proposed authentication system. A comparison between PoC2 and PoC3 reveal an increase at ZMC and USTAN, with ZMC scoring 4.37 in PoC3 (vs. 3.9 in PoC2), and USTAN scoring 4.03 in PoC3 (vs. 3.8 in PoC2), while FCRB scored lower in PoC3 with 4 (vs. 4.75 in PoC2). The overall score did not significantly change from PoC2 (4.1) to PoC3 (4.15).

#### 4.1.3.5 KPI 3.5 Patient Trust

The goal of this KPI is to measure the trust that patients have in how their data is stored and shared. We are interested in this as a metric as there is a chance that the solution is less trusted than the existing systems and thus be less likely to be opted into by patients. We evaluated this by asking several questions on the level of trust they have in the current system. These questions are e.g. *'How comfortable (1) or uncomfortable (5) would you be with this system managing your medical data?'* and '*Please rate your agreement with the following statement: "I trust this system to handle my medical data from other countries in Europe in a safe and secure manner"'*. The aim is to get an average score for all questions above 3 (50%).

| | **ZMC** | **FCRB** | **USTAN** | **TOTAL** |
|---|---|---|---|---|
| **PoC3 score** | 4.08 | 2.99 | 3.05 | 3.37 |
| **PoC3 AMPI** | 77 | 50 | 51 | 59 |

**Table 37 KPI 3.5 Patient Trust**

We can see that FCRB and USTAN both barely trust the system above the expected 3.0 value, while ZMC scores high at patient trust. In case of ZMC, there is a higher score due to the experience with the existing system of ZMC. When comparing the results with PoC2, we see a significant increase from 25. This is largely due to having a completely integrated system in place.

#### 4.1.3.6 KPI 3.6 Data Analytics Model Utility

To be in line with the subjective nature of S3, this KPI was redefined to measure the caregiver's perceived model utility and perceived model privacy with the aim to receive feedback from caregivers at ECC on the usability, utility and privacy of the toxicity predictive data models developed for the USTAN User Story (see chapter 2.3). Unfortunately, due to time constraints, the integration of the predictive data models needed to be delayed until after the PoC from March to April 2022. This meant that there was insufficient time to replan appointments with the caregivers to retrieve feedback on this system.

#### 4.1.3.7 KPI 3.7 Perceived Usability of SERUMS System

In PoC2 we have included a new KPI for measuring users' perceived usability of the SHCS system with the aim to receive feedback from end-user patients on important usability dimensions such as perceived usefulness and perceived ease of use towards the complete SHCS system. For this purpose, a questionnaire was designed following state-of-the-art works and guidelines on usability, user experience and behavioural intention to use (*i.e.*, [13]).

Regarding perceived usefulness, following the work reported in [13], we have asked questions such as, *"Using the SERUMS technology would make it possible to share and get insight in the patient's medical data"*, *"Using the SERUMS technology would make finding and sharing the patient's medical information more efficient"*, *"Using the SERUMS technology would enhance my ability to retrieve and share all patient's medical files"*, etc. Users rated the statements through a 5-point Likert scale (e.g., 1: Strongly disagree - 5: Strongly agree).

Regarding perceived ease of use, following the work reported in [13], we have asked questions such as, *"Learning to operate the SERUMS technology would be easy for me"*, *"I would find it easy to get the SERUMS* *technology to do what I want it to do"*, *"I would find the SERUMS technology easy to use"*, etc. Users rated the statements through a 5-point Likert scale (e.g., 1: Strongly disagree - 5: Strongly agree).

Regarding the behavioural to use, following the work reported in [13], we have asked the following questions: "I *would intend to use the SERUMS technology when I need access to my medical files from my native country"* and *"I would intend to use the SERUMS technology when I need access to my medical files from hospitals across Europe"*. Users rated the statements through a 5-point Likert scale (e.g., 1: Strongly disagree - 5: Strongly agree).

Based on the literature, the average SUS score is 68% [9, 10]. In case the score is significantly under 68%, the system entails various usability issues that need improvement, while a score around and above 68%, indicates that the system entails good usability practices. We strive to reach at least 70% with the SERUMS System. Top scores for usability are considered 80%.

| | **ZMC** | **FCRB** | **USTAN** | **TOTAL** |
|---|---|---|---|---|
| **Perceived Usefulness** | 4.44 | 4.49 | 4.37 | 4.43 |
| **Perceived Ease of Use** | 4.27 | 4.50 | 4.30 | 4.35 |
| **Behavioural Intention of use** | 4.17 | 4.44 | 4.42 | 4.35 |
| **Combined PoC3 Score** | 4.32 | 4.48 | 4.35 | 4.38 |
| **PoC3 AMPI** | 83 | 87 | 84 | 85 |

**Table 38 KPI 3.7 Perceived Usability of SERUMS System**

| | **Low** | **Moderate** | **High** |
|---|---|---|---|
| ZMC | 1 | 2 | 26 |
| FCRB | 0 | 2 | 15 |
| USTAN | 0 | 5 | 27 |
| Total | 1 | 9 | 68 |

**Table 39 KPI 3.7 Perceived Usability of SERUMS System - Specific results on how many patients viewed the system as useful.** ***(Low is seen as a score between 1.0 and 2.3, Moderate between 2.4 and 3.6, and High between 3.7 and 5.0)***

Overall, patients at all three end-user organisations score high on the perceived usability. The system is straight forward for the patients. We noted that ZMC was the only end-user that showed a significant increase in perceived usability in SERUMS (from 77 to 83), while the other two partners showed a slight decrease. This resulted in an end score that is only slightly higher than during PoC2 (84). The reason behind the high increase for ZMC is that sharing medical data is an unknown phenonium and was fully shown in PoC3.

### 4.1.3.8 KPI 3.8 Perceived Data Ownership in the SERUMS System

In PoC2 we have included a new KPI for measuring users' perceived data ownership when using the SHCS system. For this purpose, we have designed a questionnaire by following state-of-the-art works and guidelines in the field of usable privacy and security (*i.e.*, [14]).

Following the work reported in [14], we have asked questions such as, *"I believe the patient's personal medical information is accessible only to those authorised to have access"*, *"I think the patient has control over what personal information he or she can share via SERUMS"*, etc. Users rated the statements through a 5-point Likert scale (e.g., 1: Strongly disagree - 5: Strongly agree). Scores of 3.5 (70%) and above indicated good levels of perceived data ownership.

| | **ZMC** | **FCRB** | **USTAN** | **TOTAL** |
|---|---|---|---|---|
| **PoC3 score** | 4.22 | 4.46 | 4.30 | 4.33 |
| **PoC3 AMPI** | 81 | 87 | 82 | 83 |

**Table 40 KPI 3.8 Perceived Data Ownership in the SERUMS System**

| | **Low** | **Moderate** | **High** |
|---|---|---|---|
| **ZMC** | 1 | 4 | 24 |
| **FCRB** | 0 | 2 | 15 |
| **USTAN** | 0 | 5 | 27 |
| **Total** | **1** | **11** | **66** |

**Table 41 KPI 3.8 Perceived Data Ownership in the SERUMS System - Specific results on how high patients perceive their data ownership in SERUMS.** ***(Low is seen as a score between 1.0 and 2.3, Moderate between 2.4 and 3.6, and High between 3.7 and 5.0)***

Like the perceived usability of the SERUMS system, we see that in all patients from the three end-user organisations have a high perceived data ownership in the system. During the execution of the PoC, we were able to clearly explain what the functionality system does and how a patient is always in control of their own data. Again, it was noted that there was a significant increase in the perceived data ownership for ZMC (from 73 to 81), while USTAN had a similar score (from 84 to 82) and FCRB showed a decrease (from 92 to 87), since the score in PoC2 was very high. Overall, this resulted in good end-score for PoC3 (83). The decrease of FCRB is not alarming since the score in PoC2 was high and still is.

#### 4.1.3.9 KPI 3.9 Perceived Security in the SERUMS System

Following state-of-the-art user studies in usable security research [11, 12], for perceived security, we have asked participants questions on whether they believe the overall SHCS system is secure. Example questions include *"Overall, how secure do you find the SERUMS system?"*, *"I am not worried about the security of the SERUMS system"*, etc. Users rated the statements through a 5-point Likert scale (*e.g.*, 1: Very insecure - 5: Very secure). Scores of 3.5 (70%) and above indicated good levels of the perceived security.

| | **ZMC** | **FCRB** | **USTAN** | **TOTAL** |
|---|---|---|---|---|
| **PoC3 score** | 3.97 | 4.19 | 4.13 | 4.10 |
| **PoC3 AMPI** | 74 | 80 | 78 | 77 |

**Table 42 KPI 3.9 Perceived Security in the SERUMS System**

| | **Low** | **Moderate** | **High** |
|---|---|---|---|
| **ZMC** | 3 | 5 | 21 |
| **FCRB** | 1 | 2 | 14 |
| **USTAN** | 2 | 8 | 22 |
| **Total** | 6 | 15 | 57 |

**Table 43 KPI 3.9 Perceived Security in the SERUMS System - Specific results on how many patients viewed the SERUMS system as sure. *(Low is seen as a score between 1.0 and 2.3, Moderate between 2.4 and 3.6, and High between 3.7 and 5.0)***

Again, we see that in all patients from the three end-user organisations have a high perceived data ownership in the system. However, while most patients still had high perceived security in the SERUMS system, it is noted that there were more people who did not have a high score compared to perceived usability and perceived data ownership. Compared to PoC2, we noted that there was again a significant increase for ZMC (from 68 to 74), while USTAN showed a slight increase (from 76 to 78) and FCRB showed again a significant decrease (from 87 to 80). Overall, this resulted in good end-score for PoC3 (77).

### 4.1.4 Success Indicator 4

Success Indicator 4 aims to improve the patient safety, 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. To accomplish it, we developed innovative technology to deal with level of accuracy between different models.

#### 4.1.4.1 KPI 4.1 Data Analytics Model Utility

Like the privacy models discussed in KPI 4.1.2.3, when developing privacy-preserving machine learning models there is always a trade-off between a model's privacy and a model's utility, and thus it is necessary to define the level of accuracy of the models.

To evaluate privacy-preserving machine learning methods, a ratio, measuring the loss in accuracy as of decreasing privacy-loos bound for a fixed failure probability, is defined. The fabricated USTAN use case dataset was used to evaluate the developed methodology and compared to the state-of-the-art machine learning methods. The best performing existing machine learning method together with the optimised differentially private noise adding mechanism was considered as the reference method for a comparison.

It is observed that the developed methodology resulted on the fabricated USTAN use case dataset in a gain of accuracy by a factor of 2.1121 over the reference benchmark method. Due to the logarithmic nature of factorial increases, this resulted in an AMPI score of 66.

# 4.2 Evaluation: Use Case perspective

## 4.2.1 Evaluation: ZMC

As mentioned before, we had to shift the execution of our Proof of Concept from a hybrid execution (both digital and physical) to a completely digital execution. The recruitment of participants partially took place via the medical staff of the department involved in the SERUMS project, since they treat patients representing the use case. In addition, we asked the coordinators of the Zuyderland Panel representing the older population and the Zuyderland Client Board to inform their members. Since we were in lockdown, everything had to be organised online by using email and Microsoft Teams. Therefore, it took more time than initially planned to recruit participants and execute the interviews. In addition, it sometimes took a few days to eventually obtain the informed consent. Therefore, to make sure enough participants were included, the execution period of PoC3 was extended to 4 weeks. We managed to recruit 31 patients. Unfortunately, in 2 situations, the patients were unable to get a connection with the interviewer using Microsoft Teams. So, the results of 29 patients, ranging in age from 24 to 79, were included in the research. In addition, we interviewed 4 medical professionals and organised a focus group where 3 IT specialists from ZMC participated.

Most of the participants were familiar with using Microsoft Teams. Once the FlexPass password was created, participants were asked to share their screen with the interviewer. In this way, the interviewer could observe, give instructions where necessary and offer help when problems occurred. In one interview with a doctor and in two interviews with patients the SHCS did not show patient data. Therefore, the interview with the doctor was postponed and resumed later within the 4 weeks during PoC3. In the case of the 2 patients there was one time where we could solve the problem by restarting the login procedure and in the other case the interviewer logged into the system and then shared the screen so that the patient data could still be shown, and the participant experienced what this looked like. Some of the participants running the platform on their iPad experienced difficulties in creating the picture password. For these participants, an average of 5 attempts was needed to finally create the password. The main outputs of PoC3 can be outlined as follows:

- Overall, during the interviews, most participants expressed their enthusiasm for the system and said they would look forward using a similar system soon. The answers to the open questions in the questionnaire also showed that the patients trust the system and value the possibility of controlling who has access to their medical files. One patient mentioned that they needed the SERUMS system a few years ago when they were hospitalised during a holiday in France. Most participants also indicated that they experience the FlexPass system as secure and user-friendly, although the creation of a picture password on an iPad still needs improvement.
- The doctors were excited about the possibility to share medical data to or obtain from caregivers from other organisations (abroad). Even a document written in a foreign language did not matter to them that much, as they stated that they can use translation tools to help them understand the content. They were especially pleased with the option to request access to specific data, which they feel is necessary.
- The IT focus group was very interested in several innovative techniques such as data fabrication and predictive models. As cure and care are shifting more towards home the need for gathering and sharing medical data on patients from various sources is becoming more important. The temporary nature of the Data Lake and its structure were considered therefore valuable as patients will be monitored in a Hospital Control Centre within the next decade.

ZMC has some challenges ahead such as: i) a digital transformation and further development in providing (remote) healthcare, ii) building a new (smart) hospital before 2030, and iii) meeting the obligations of the Dutch legislation and regulations regarding medical data sharing. Our IT staff members evaluated the solutions and technologies used in the Serums system during the IT-focus group and they see possibilities to use some of it shortly to support these transformations.

## 4.2.2 Evaluation: FCRB

Due to the 4th wave of Covid-19 virus in Spain, the inclusion and interview sessions could not take place physically but needed to take place virtually. This made recruitment planning and execution hard. We therefore needed to extend the period of PoC3 to three weeks. The process of obtaining ethical consent was delayed, as several internal meetings of the Ethical Committee were cancelled or delayed due to Covid-19. Even with the extension and the help of the Diabetes Medical Specialist, we were only able to recruit 21 participants from ages 25 to 75 (some of them already participated in the previous PoCs). In addition, we included 2 medical staff.

As mentioned, the interviews were conducted online through Microsoft Teams. Participants were asked to share their screen with the interviewers after the FlexPass password creation (due to privacy reasons). Following, they shared the screen for testing the SHCS, which allowed support to be offered if required and allowed early identification of any doubt or issue. In the first days of the studies, some minor issues were spotted and fixed. Additionally, one patient experienced more difficulties using the FlexPass graphical password as she was running the platform on the iPad. However, in the end she could set up the password.

The main outputs of the third PoC are:

- Overall, all the patients liked the possibility of controlling the access to their medical records. Many of the participants liked the use case of cross-border sharing, as there is not an easy platform to do so.
- The doctors were willing to use the system, they liked the possibility sharing the data from Caregivers from other organisations. Although some UI improvements need to be made. Overall, they saw the platform could help to understand more the patient, because of a having a unique platform of access medical records.
- Patients found the questionnaire quite long, occasionally confusing, and sometimes repetitive, in specific sections; some participants needed assistance with some questions wording.
- In general terms, participants overwhelmingly trusted the system despite PoC3 being executed completely remotely and only a few participants were not familiar with technologies such as 'Teams meetings', screen sharing feature and video/audio options.

### 4.2.3 Evaluation: USTAN

A total of 32 participants, ranging in age from 26 to 65, were recruited via social media for the final PoC in Scotland, UK. This included 28 potential patients, one member of medical personnel (a doctor) and three IT staff members. All participants were from the area local to the University of St Andrews. Interviews were conducted over Teams or Zoom during a week-long period spanning from 23rd March until 1st April 2022.

The overall public feedback on the system during the sessions was good or very good, people liked the idea of the system, having a platform to share their medical data, which allowed them to visualise their own data in some way. Additionally, they were positive about having the ability to grant access to their data in the future.

Most of the feedback received was centred on the authentication module, for example installing the app for the 2F authentication - some lacked enough memory on their phones and needed to first uninstall personal apps to enable installation of the SERUMS authenticator. This was seen as a barrier to using the app in few cases.

During the PoC, there were two cases where people uninstalled the app immediately after answering the questionnaire, resulting in issues to run the post-study. This was resolved by restarting the system to enable these participants to proceed. Besides this, no major issues were reported.

A small number of participants (2) attempted to carry out the post-study using their mobile phones or tablets and had issues performing the gestures to login using picture password. This issue was only resolved when they contacted the team and were advised to reattempted login using their PC.

Regarding other important features, such as access rule creation, there was great acceptance on this functionality, especially relating to the way in which the rules are created. Gained feedback suggested that users found the format of this rule creation mechanism to be straightforward, with clear information for the front-end user. However, a few described that they would prefer the responsibility for requesting rules to fall to their medical practitioner, rather than to the patients themselves.

Overall, there was a positive public outcome to performing the PoC3, with encouraging feedback. Participants described having high levels of confidence in the system and its ease of use, as defined by the tasks they were asked to perform in the system.

## 4.3 Discussion

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. The overall results, shown in Table 44, show an improvement in all four Success Indicators. The following paragraphs will elaborate on the impact of the system.

| Impact | **Success Indicator** | **Baseline** | **Benchmark** | **PoC 1** | **PoC2** | **PoC3** |
|---|---|---|---|---|---|---|
| **I** | **Quantifiable improvement in the secure provision of health and care services** | | | | | |
| | **S1** | 45 | 64 | N/A | 61 | 71 |
| **II** | **Impact II: Significantly reduced risk of data privacy breaches** | | | | | |
| | **S2** | 38 | 70 | N/A | 58 | 80 |
| **III** | **Increased patient trust and safety** | | | | | |
| | **S3** | 70 | 68 | 74 | 74 | 77 |
| | **S4** | N/A | 50 | N/A | N/A | 66 |

**Table 44 Success Indicators**

### 4.3.1 Security

The impact, measured with Success Indicator 1, to be made was defined as improved security of Health and Care services, data, and infrastructure. As can be seen in Table 44, Success Indicator 1 showed an improvement between PoC2 and PoC3, and the benchmark was reached in PoC3. Both KPI 1.1 Guessability and KPI 1.2 Password leaks showed an improvement and exceeded the benchmark. For example, memory time (part of KPI 1.2) scored good (133.5/168 in hours), which suggests that end-users were able to effectively recall their passwords over a period of one week.

Even though the targets for this success indicator have been met, KPI 1.3 System Vulnerability did not exceed the expected benchmark (63). This might be due to the sensitive nature of the data, since not all use case partners were able to provide data for all survey questions. In Scotland, the medical data is controlled by the NHS, whereas in the Netherlands and in Spain the medical data is controlled by each hospital.

### 4.3.2 Data privacy breaches

The impact, measured with Success Indicator 2, to be made was defined as less risk of data privacy breaches caused by cyberattacks. First, as can be seen in Table 44, the set benchmark for Success Indicator 2 was reached. Thereby, all individual KPIs showed an improvement, and all benchmarks were reached, or exceeded.

A striking result regarding Success indicator 2 is the KPI 2.1 Password Cracking Resistance. Typically, rates for normal password distributions allow for a password cracking rate of around 51.80%. During PoC3, several technological and practical attempts were made to guess a password, but all attempts were unsuccessful. This shows that the security of the key is high.

One remark regarding the outcomes of Success Indicator 2, is that the technical component of the blockchain was not ready to be demonstrated to the end-user until PoC2 since the integration did not take place yet. Therefore, the measurement of these KPIs started in PoC2. Except for KPI 2.3, since the models used to measure this KPI were only available from PoC3 onwards, this KPI was only measured in PoC3. Although, since this KPI is not included in the calculation of Success Indicator 2 in PoC 1 and PoC2, we do not expect a significant effect, since the coefficient from this KPI is only a factor 1 out of 10 (see Table 6).

### 4.3.3 Patient trust and usability

The impact, measured with Success Indicator 3, to be made was a quantifiable improvement in levels of patients trust in the provision of smart health care. As can be seen in Table 44, Success Indicator 3 showed an improvement in PoC3 compared to the benchmark and the other executed Proof of Concepts. For example, the overall system usability score of FlexPass (72%) scores well, based on the guidelines of the System Usability Scale (SUS), which suggests that a score above 68% indicates good usability practices. Areas for improvement relate to the graphical password gesture input functionality on heterogeneous devices through responsive design mechanisms. One remark on the outcomes of Success Indicator 3 is that KPI 3.6 could not be measured during these PoCs. Due do time constraints, we were not able to include KPI 3.6 in interviews and therefore, no data was available for this KPI. To avoid influencing the outcome, the KPI is not included in the calculation of the Success Indicator. Although, due to the high margin difference between the benchmark and the outcome of PoC 3, we do not expect this to have a significant impact.

Concerning the authentication technology (FlexPass), KPIs reveal similar values in PoC3 compared to PoC2, with the personalised images. Therefore, further investigation is suggested to the personal user authentication approach. Results indicate a continuation of KPI 3.1 (Perceived Usability), KPI 3.2 (Perceived Memorability), KPI 3.3 (Perceived Security) and KPI 3.4 (Trust in the Proposed PUA Scheme) towards the SERUMS authentication technology. In addition, the user authentication technology revealed that providing personalised images to patients leads to increased security in terms of number of guesses required to crack a password compared to generic images that are not familiar to the end-users. Furthermore, regarding the SERUMS Two-Factor Authentication (2FA) application, at PoC2 only 22% of participants had used but in PoC3 most of the participants (85%) downloaded and used the mobile application. We also have measured a push notification accuracy of a 100%.

Regarding the usability of the system, most participants indicated a high usability (88%). 11% of participants indicated the usability as medium, and only 1% perceived it as low. When users were asked about the overall security, 74% of the users perceived the security as high, 19% of the participants answered medium, and only 7% experienced the security as low. This indicates that overall, the SERUMS system was thought to be secure and easy to use.

### 4.3.4 Patient Safety

The impact, measured by Success Indicator 4, to be made was quantifiable improvement (benchmark 50) in patient safety, 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 systems. Unfortunately, S4 could not be measured during PoC1 and PoC2, because the Machine Learning was not yet implemented. In PoC3, we were able to measure KPI 4.1. that showed successful results regarding data privacy.

It is observed that the developed methodology resulted on the fabricated USTAN use case dataset in a gain of accuracy by a factor of 2.1121 over the reference benchmark method. Due to the logarithmic nature of factorial increases, this resulted in an AMPI score of 66 and means that we reached the proposed impact.

# 5 Conclusions

This deliverable presents the work performed during the third phase of the demonstration of the SERUMS technologies' effectiveness. More specifically:

- It evaluates the final prototypes of the SERUMS technologies developed against the overall project requirements and success criteria that were refined/updated in D7.4.
- It reports the progress achieved in the different Success Indicators compared to the work performed during the first phase and presented in D7.3 and in the second phase on D7.5.

Despite the Covid-19 pandemic, we were able to conduct a decent PoC3. Although all was done digitally and many patients were of old age, we experienced very few problems with screen-to-screen interviews and screen sharing. In addition, looking back at the three Proof of Concepts, we see an improvement during each phase. In the first phase the integration of the SERUMS Technologies was not achieved yet. In the second phase an initial integrated and coherent version was implemented and tested. Last, the third phase showed a completed integrated system, where patients and staff get a glimpse of what might be in the future, which is reflected in the results.

As presented in paragraph 4.3 'Discussion' all four Success Indicators met their benchmark, thus the expected impact has been achieved. In addition, the objectives reported in the proposal 'Securing Medical Data in Smart Patient-Centric Healthcare Systems, April 25, 2018', are achieved:

1. The combination of techniques like data lake, data masking and blockchain ensures the security and protection of personal medical data that is shared as part of a coherent smart healthcare system between patients, hospitals, and medical practitioners, including across (possibly open and/or public) untrusted networks.
2. Measurements from various sensors, doctors' letters, x-rays, and medical hospital data are stored in a single coherent smart patient record.
3. With data fabrication, privacy preserving analytics and blockchain rules we are able to take advantage of advances in the availability of heterogeneous real-time personal healthcare information, as part of a holistic smart healthcare system, while respecting privacy and security concerns.
4. Easy to use authentication mechanisms have been developed (FlexPass system) to ensure only authorised persons have access to the SERUMS system. Through access rules controlled by Blockchain technology patients can admit or revoke access to (parts of) their medical data. The hospital admin of the SERUMS system controls which staff member belongs to which department (e.g., emergency, surgery, orthopaedics, etc.).
5. As patients are in control of whom to share their medical data with or not, and the complementary audit trail from the Blockchain technology, compliance with emerging legal and ethical requirements for the protection of personal and medical data across national boundaries, including transnational requirements such as GDPR is established
6. We have conducted three PoCs at the three end-user organisations to test the effectiveness of the SERUMS techniques against a variety of real-world medical use cases, including both ongoing and emergency medical care scenarios, providing confidence in the delivery of high quality, ethically and legally compliant smart healthcare.
7. Although this objective is not part of this deliverable, it is value to mention that, as presented in D8.8 (Final Report on Dissemination & Exploitation, including Exploitation Plan, Communication Activities, User Community Building, IPR Management, and Final Project Workshop'), a good uptake of SERUMS concepts and technologies that targets potential users of smart healthcare systems, as well as leading technology and healthcare providers, is ensured.

Thus, our findings show that, from a technical standpoint, we have achieved our initial proposed impact based on the Success Indicators. Our technical KPIs show similar or better scores than our benchmark measurements. These scores also helped us identify areas that can be improved. In the current state, the SERUMS system is not ready yet to be made available to the public, as various functionalities need to be further developed to be ready for upscaling of use. Next steps (discussed in detail in D7.7 Report on Technical Roadmap for SERUMS Technology) include developing several functionalities to facilitate international data exchange and to facilitate hosting across multiple locations. It is planned to investigate alternative authentication methods for visual impaired users, such as audio recognition or other initiatives towards a more accessible authentication scheme, to ensure the SERUMS system would be available to as many people as possible.

# 6 References

[1] 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

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

[3] 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

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

[5] 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

[6] Zhao, Z., Ahn, G.J. and Hu, H., 2015. Picture gesture authentication: Empirical analysis, automated attacks, and scheme evaluation. ACM Transactions on Information and System Security (TISSEC), 17(4), pp.1-37.

[7] Stobert, E., & Biddle, R. (2013). Memory retrieval and graphical passwords. In Proceedings of the symposium on usable privacy and security (p. 15). ACM

[8] Constantinides, A., Fidas, C., Belk, M., Pietron, A., Han, T., Pitsillides, A. (2021). From hot-spots towards experience-spots: Leveraging on users' sociocultural experiences to enhance security in cued-recall graphical authentication. International Journal of Human-Computer Studies, Elsevier, 149, 102602

[9] John Brooke. 1996. SUS-A quick and dirty usability scale. Usability evaluation in industry 189, 194: 4--7.

[10] John Brooke. 2013. SUS: A Retrospective. J. Usability Studies 8, 2: 29--40

[11] Sonia Chiasson, P. C. van Oorschot, and Robert Biddle. 2006. A usability study and critique of two password managers. In Proceedings of the 15th conference on USENIX Security Symposium - Volume 15 (USENIX-SS'06). USENIX Association, USA, Article 1, 1.

[12] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. 2019. A usability study of five two-factor authentication methods. In Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security (SOUPS'19). USENIX Association, USA, 357–370.

[13] Fred D. Davis. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q. 13, 3 (September 1989), 319–340. DOI: https://doi.org/10.2307/249008

[14] Oshrat Ayalon and Eran Toch. 2019. Evaluating users' perceptions about a system's privacy: differentiating social and institutional aspects. In Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security (SOUPS'19). USENIX Association, USA, 41–59.

# 7 Abbreviations

| | |
|---|---|
| 2FA | Two-Factor Authentication |
| AM | Activity Monitor |
| CH | Credential Hardening |
| DLT | Distributed Ledger Technology |
| ECC | Edinburgh Cancer Centre |
| FlexPass | The SERUMS user authentication technology |
| GDPR | General Data Protection Regulation |
| KPI | Key Performance Indicators |
| MNIST | Modified National Institute of Standards and Technology |
| PDA | Privacy-preserving Data Analytics |
| PHE | Personal Health Environment |
| PoC | Proof of Concept |
| PoC2 | second Proof of Concept |
| PoC3 | third Proof of Concept |
| PROMS | Patient Reported Outcome Measures |
| PUA | Personalised User Authentication |
| SHC | Smart Health Centre |
| SI | Success Indicator |
| SPR | Smart Patient Record |
| SUS | System Usability Scale |
| VOT | Verification Technologies |
| WGH | Western General Hospital |

# 8 Appendix

## Appendix 1 - participant information letter

What is the study about?
We invite you to participate in a research project about Securing Medical Data in Smart Patient-Centric Healthcare Systems (SERUMS) which deals with security and privacy of future-generation healthcare systems, putting patients at the centre of future healthcare provision, enhancing their personal care, and maximizing the quality of treatment they receive.

Why have I been invited to take part?
The main purpose of this study is to elicit the end-users opinions, preference, and likeability with regards to FlexPass, a novel user authentication system that aims to improve usability and memorability of passwords and at the same time preserve security.

Do I have to take part?
This information sheet has been written to help you decide if you would like to take part. It is up to you and you alone whether you wish to take part. If you do decide to take part you will be free to withdraw at any time without providing a reason, and with no negative consequences.

What would I be required to do?
Today you will test that system by performing several tasks in it. Afterwards you will be provided with a questionnaire that will ask your opinion. Please be honest, as your opinion can still cause us to improve the system in the last phase of the project.
The user study will take about 45-75 minutes. Your answers will be treated confidentially and anonymously
Part 1: You will interact with the Proof of Concept (PoC) Web-based authentication system by creating a password and then logging into the system.
Part 2: You will then be given a PoC questionnaire to get feedback on aspects like perceived usability, security, acceptance, and trust towards the PoC authentication system.
After the study, we will send you three notification emails on Day 1, Day 3, and Day 6. Each email will direct you to the SERUMS system and it will instruct you to access the system

Are there any risks associated with taking part?
There are no risks to individuals participating in this study beyond those that exist in daily life.

Informed consent
It is important that you are able to give your informed consent before taking part in this study and you will have the opportunity to ask any questions in relation to the research before you provide your consent. For further questions about this study, the project or about the way your contribution will be used, please feel free to contact us.

Who is funding the research?
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826278.
For more information about the project, please visit the project's official Website: www.SERUMS.h2020.org

What information about me or recordings of me ('my data') will you be collecting?
We will explicitly collect your opinions with regards to the user authentication scheme questionnaires to measure the perceived usability, memorability, security, and trust with regards to the user authentication scheme.

During user interaction, we will track the following data for the purpose of the project. *All the data will be anonymously stored without any binding information to the identity of the participants*:
User Interaction and Usage Data

- Authentication usage data: i) timed events of user interaction, i.e., time to create each gesture (seconds), time to create password (seconds); ii) number of attempts to create and confirm password (ordinal); iii) time to login (seconds); iv) number of attempts to login (ordinal); and v) second factor response (true/false) along with the timestamp of occurrence.
- Authentication memory data: i) memory time (seconds) which is the greatest length of time between a password creation and a successful password login using the same password; ii) number of password resets (ordinal).
- False Acceptance Rate of 2FA: the percentage of identification instances in which unauthorised persons are incorrectly accepted.
- False Rejection Rate of 2FA: the percentage of identification instances in which authorised persons are incorrectly rejected.
- Effectiveness of 2FA: Percentage of sent push notifications that arrived at the correct smartphone.
- Failure to Enrol to 2FA: The percentage of the population which fails to complete enrolment of the mobile application.

User-created Password Data

- Security-enhanced textual and graphical password data based on credential hardening.
- Selected images of the recognition-based picture password without any binding information to the identity of the end-user.
- Gesture type (i.e., tap, line circle) and selections on a background image (i.e., x, y coordinates, image semantics of the selection, whether the selection is a hotspot vs. non-hotspot region) of the recall-based picture password without any binding information to the identity of the end-user.

We will securely store email address for the follow up for the memorability evaluation your email will be stored at our organisation for a period of 7 days after your participation, and it will be then deleted permanently. Your email will be used solely for the purpose of sending the above-mentioned 3 notification emails for instructing you only to access the SERUMS system.

How will my data be securely stored, who will have access to it?

Your data will be stored in an anonymised form, which means that parts of your data will be edited or deleted such that no-one, including the researchers, could use any reasonably available means to identify you from the data. Your un-anonymised data will then be permanently deleted. Your data will be stored in secure location, and only relevant members on the project will be able to access it.

How will my data be used, and in what form will it be shared further?

Your research data will be analysed as part of the research study. It will then be used in various research publications and in the project Reports. It will also be shared i.e., by placing it in a database accessible by other members of the consortium. All data will be anonymised for processing, which means that no-one could use any reasonably available means to identify you from the data and will be stored on a secure server which will be encrypted.

When will my data be destroyed?

Data will only be used during the duration of the project which will end on Dec 2021 and will be destroyed.

International data transfers – Personal data

No identifiable data will be shared. Only anonymised data based on user opinion will be shared and stored by other members of the group in Barcelona, Cyprus, and The Netherlands where it will be stored on a secure encrypted server.

Will my participation be confidential?

Yes, your participation will only be known to the relevant members on the project. This data will be kept only for the use of the project and will not be shared out with the members of the consortium.

Use of your personal data and data protection rights

The University of St Andrews (the 'Data Controller') is bound by the UK 2018 Data Protection Act and the General Data Protection Regulation (GDPR), which require a lawful basis for all processing of personal data (in this case it is the 'performance of a task carried out in the public interest' – namely, for research purposes) and an additional lawful basis for processing personal data containing special characteristics (in this case it is 'public interest research'). You have a range of rights under data protection legislation. For more information on data protection legislation and your rights visit https://www.st-andrews.ac.uk/terms/data-protection/rights/. For any queries, email dataprot@st-andrews.ac.uk.

Ethical Approvals

This research proposal has been scrutinised and subsequently granted ethical approval by the University of St Andrews Teaching and Research Ethics Committee.

What should I do if I have concerns about this study?

In the first instance, you are encouraged to raise your concerns with the researcher. However, if you do not feel comfortable doing so, then you should contact The School of Computer Science Ethics Administrator. Ethics-cs@st-andrews.ac.uk A full outline of the procedures governed by the University Teaching and Research Ethics Committee is available at https://www.st-andrews.ac.uk/research/integrity-ethics/humans/ethical-guidance/complaints/.

For more information about the project, please visit the project's official Website: www.SERUMS-h2020.org.

Thank you for taking your time to support this project!

Contact details

| | | |
|---|---|---|
| **Researcher(s)** | School Ethics contact | School of Computer Science<br>01334 463273 |
| Dr Juliana Bowles[jkfb@st-abndrews.ac.uk]<br>Dr Thais Webber [tcwds@st-andrews.ac.uk]<br>Guilherme Redeker [gr60@st-andrews.ac.uk]<br>Agastya Silvina [as362@st-andrews.ac.uk] | | |

# Appendix 2 - instructions for participants

## Instructions for users

Thank you for participating in this user study for the EU Horizon 2020 research project SERUMS.

The main purpose of this study is to evaluate the user friendliness, usability, and security of the system, as well as to collect end-user opinions regarding SERUMS. This is a system that offers patients and healthcare providers a central place to view and store medical data. It includes a new authentication system, called FlexPass, which aims to improve the usability and "memorability" of passwords while maintaining security. In addition, it includes a central place to view your medical records from anywhere in Europe and allows you to set up permissions and restrictions on who can and cannot see your data.

Today you will test that system by performing various tasks in it. Then you will be given a questionnaire that will ask you for your opinion. Please be honest because your opinion can help us get proper insight into the system.

### About FlexPass

FlexPass is a user authentication system that allows users to create photo passwords. Instead of remembering complex text passwords, you only need to remember 3 secret spots on an image by drawing them on the image.

To make your picture password more memorable, secure, and easier to use, FlexPass provides pictures that are tailored to each user's previous activities and experiences in daily life.

In addition, if you want to use textual passwords, you can also create a secret password called passphrase that allows you to flexibly switch between your picture password to log in.

Finally, to add an additional layer of security, users have the option to install a mobile application, which is used as a second authentication factor through an easy-to-use push notification, with the aim of increasing the security of the login task.

### Study Procedure Instructions

For the study, we ask you to imagine yourself as Peter, an orthopaedic patient at Zuyderland Medical Centre. You have just been to the hospital for a hip replacement. For your own benefit and your future treatment plan, you would like to gain insight into your medical data and share it with your physiotherapist. To do this, you will use the Serum system. Below are the main steps you need to follow to perform this action. Next, a questionnaire will begin to ask you some questions about the system.

### Step 1 – Create Picture Password

1. Click on the Sign-up button; a username will be provided to you during the Microsoft Teams' meeting.
2. A set of background images will be displayed on the screen. The images will depict content that you are familiar with. You are required to select one image from the set of images, on which you will then create your picture password.
3. Next, you will create a picture password by drawing 3 gestures on an image. You could use any combination of circles, straight lines, and taps (clicks).

4. Memorise the size, the position, the directionality, and the ordering of your gestures. These gestures will be your secret picture password.

**Step 2 – Create Textual Password (optional)**

In case you like to use textual passwords, you can also create a secret passphrase (minimum 16 characters long), which you can use to flexibly switch between your picture password in order to login.

In order to make your password more memorable, we suggest reflecting the secret you created in the picture password as your passphrase. For example, *“the day I had lunch with my friends at the cafeteria”*.

**Step 3 – Setup Second Factor for Authentication – requires installation of mobile application**

In case you would like to make the access to your account more secure, you could set up an additional authentication factor by receiving a push notification during login on your mobile device.

In order to make access to your account more secure, we strongly encourage you to set up the second factor for authentication.

**Step 4 – Login and Approval**

In order to login in the system, you need to choose your preferred authentication method (picture or text) and then proceed to login by entering your secret password.

If you selected a second factor for authentication for increased security during the login process, you also need to approve your login through a push notification that will show up on your mobile device.

**Step 5 – Find your medical information**

In order to be able to share the necessary medical data with your general practitioner, you need to know where it is. Access your Smart Patient Record (SPHR) to find the information about diagnosis and personal information.

**Step 6 – Find your treatment data**

You also want to consult the information available on your upcoming treatments. Please find the information and view the details.

**Step 7 – Allow a healthcare department to see your data**

You want to share your general medical information and diagnosis, for instance, with the general practitioner (GP) or other professional of your choice. Please allow the professional to see your data.

**Step 8 – Deny your acquaintance to see your medical data**

Within the orthopaedics department you have an acquaintance which you rather would not share your data with. Please deny a specific professional access to all of your data.

**Step 9 – Allow a healthcare provider from Spain to see your medical data**

During your vacation, your hip starts hurting again. Because the operation was a few weeks ago, you visit the nearest first aid department of a hospital in Barcelona to let it check out. Please give the Spanish hospital FCRB access to all your medical data.

**Step 10 – Check with your interviewer what you have given access to**

Ask you interviewer to log in as the caregiver from the Spanish hospital FCRB and look together at which medical data is visible for FCRB and how it looks.

**Step 11 – Make the Spanish report available for your Dutch doctors and check it**

After treatment in Spain, the doctor asks you to share the results with your doctors at home. Please allow Zuyderland and your GP access to the medical data from the Spanish hospital FCRB. Afterwards, ask your interviewer again to see the report.

### Last Step 12 – Questionnaire

In the last step, please answer a questionnaire to indicate your opinions, preference, and likeability with regards to SERUMS' system.

# Appendix 3 - questionnaire for patients

**Thank you for taking your time to support this project!**

## Consent

By clicking the "Next" button you declare that you

1. understand the purpose of the study,
2. are over 18 years old,
3. voluntarily participate in this study, and
4. have taken note and understand the study information presented above.

## User ID

1. Please enter your User ID that was provided by the researcher

   *Text field*

## General Background

2. What is your Age range (in years)?

   *18-25; 26-35; 36-45; 46-55; 56-65; 66 and above*

3. What is your highest degree of education?

   *Ph.D. Studies; Master Studies; Bachelor Studies; High School; Primary School*

4. How would you rate your computer literacy?

   *Beginner 1 2 3 4 5 Advanced*

5. Do you currently have regular access to a computer?

   *Yes, No*

## FlexPass Password System Usability

*Please rate the usability of the FlexPass Password System*

6. I think that I would like to use the FlexPass system frequently.

   *Strongly disagree 1 2 3 4 5 Strongly agree*

7. I found the FlexPass system unnecessarily complex.

   *Strongly disagree 1 2 3 4 5 Strongly agree*

8. I thought the FlexPass system was easy to use.

   *Strongly disagree 1 2 3 4 5 Strongly agree*

9. I think that I would need the support of a technical person to be able to use the FlexPass system.

   *Strongly disagree 1 2 3 4 5 Strongly agree*

10. I found the various functions in the FlexPass system were well integrated.

   *Strongly disagree 1 2 3 4 5 Strongly agree*

11. I thought there was too much inconsistency in the FlexPass system.

   *Strongly disagree 1 2 3 4 5 Strongly agree*

12. I would imagine that most people would learn to use the FlexPass system very quickly.

   *Strongly disagree 1 2 3 4 5 Strongly agree*

13. I found the FlexPass system very cumbersome to use.

   *Strongly disagree 1 2 3 4 5 Strongly agree*

14. I felt very confident using the FlexPass system.

   *Strongly disagree 1 2 3 4 5 Strongly agree*

15. I needed to learn a lot of things before I could get going with the FlexPass system.

   *Strongly disagree 1 2 3 4 5 Strongly agree*

## Password Creation

*Please rate your experience and perceptions with regards to the FlexPass password creation system and process*

16. Overall, how difficult or easy did you find the password creation task in FlexPass?

   *Very difficult 1 2 3 4 5 Very easy*

17. Overall, how slow or fast did you find the password creation task in FlexPass?

   *Slow 1 2 3 4 5 Fast*

18. How long (in seconds) did you need to create your password in FlexPass?

   *Text field*

19. Overall, how secure do you find the FlexPass password system?

   *Very insecure 1 2 3 4 5 Very secure*

20. How strong do you believe your FlexPass password is?

   *Very weak 1 2 3 4 5 Very strong*

21. Did the image scenery impact your password selections (i.e., did you create a certain story when selecting points on the image, did you consider any past experiences as part of your selections)? If yes, please explain how the image scenery impacted your password selections (optional)

   *Text field*

22. How did you decide where to draw the gestures on the image? (optional)

   *Text field*

23. How did you decide which gesture (tap, line, or circle) to draw? (optional)

    *Text field*

24. What strategy did you follow to create your password? (optional)

    *Text field*

25. What type of background image would you prefer? (optional)

    *Text field*

## Password Login

*Please rate your experience and perceptions with regards to the FlexPass login system*

26. Overall, how difficult or easy did you find the login task in FlexPass?

    *Very difficult 1 2 3 4 5 Very easy*

27. How mentally demanding was the login task?

    *Very low 1 2 3 4 5 Very high*

28. I could easily log on to the FlexPass password system

    *Strongly disagree 1 2 3 4 5 Strongly agree*

29. I effectively remembered my password

    *Strongly disagree 1 2 3 4 5 Strongly agree*

## Two-factor Authentication Mobile Application

*In case you have used the two-factor authentication mobile application, please rate your experience and perceptions with regards to the two-factor authentication system*

30. Did you successfully install and enrol in the two-factor authentication mobile application?

    *Yes No*

31. If your answer was "Yes", which two-factor authentication method did you use to login?

*Push notification message; Secret code (Time-based One-Time Password - TOTP)*

32. Did you successfully access the system after using the two-factor authentication method?

    *Yes No*

33. Overall, how difficult or easy did you find the installation and enrolment to the two-factor authentication mobile application?

    *Very difficult 1 2 3 4 5 Very easy*

34. Overall, how difficult or easy did you find the two-factor authentication approval task (push notification or secret code)?

    *Very difficult 1 2 3 4 5 Very easy*

35. Overall, how secure do you find the two-factor authentication mobile application?

*Very insecure 1 2 3 4 5 Very secure*

36. I would be willing to use the two-factor authentication mobile application in my everyday tasks

    *Strongly disagree 1 2 3 4 5 Strongly agree*

## Password Reset

*In case you have reset your password, please rate your experience and perceptions with regards to the FlexPass password reset system and process*

37. Overall, how difficult or easy did you find the password reset process of the FlexPass system?

    *Very difficult 1 2 3 4 5 Very easy*

38. Overall, how secure did you find the password reset process of the FlexPass system?

    *Very insecure 1 2 3 4 5 Very secure*

## Trust

*Please rate your trust towards the FlexPass password system*

39. I trust in the technology the FlexPass password system is using

    *Strongly disagree 1 2 3 4 5 Strongly agree*

40. I trust in the ability of the FlexPass password system to protect my privacy

    *Strongly disagree 1 2 3 4 5 Strongly agree*

41. I am not worried about the security of the FlexPass password system

    *Strongly disagree 1 2 3 4 5 Strongly agree*

42. I trust the FlexPass password system to protect my account and data from cybercriminals

    *Strongly disagree 1 2 3 4 5 Strongly agree*

## Password Experience and Preference

*Please explain your overall experience, preference and opinions with regards to the FlexPass password system*

43. Do you like the idea of creating picture passwords with personalised images tailored to the users' prior daily life activities and experiences?

    *Not at all 1 2 3 4 5 Extremely*

44. Do you like the idea of allowing users to flexibly choose their preferred authentication method (picture or text password)?

    *Not at all 1 2 3 4 5 Extremely*

45. What are the positive aspects you like in the FlexPass password system? (optional)

    *Text field*

46. What are the negative aspects you do not like in the FlexPass password system? (optional)

*Text field*

47. I would be willing to use the FlexPass password system as an alternative user authentication system to login to my user account

    *Strongly disagree 1 2 3 4 5 Strongly agree*

48. Explain the reasoning behind your answer in the previous question

    *Text field*

49. Do you believe that FlexPass' personalised picture passwords would potentially reveal private information of users and raise privacy concerns?

    *Strongly disagree 1 2 3 4 5 Strongly agree*

50. In case you believe that FlexPass entails privacy issues, please elaborate on these and provide preferred methods to assure privacy-preservation. (optional)

    *Text field*

## Patient trust medical data

51. How comfortable (1) or uncomfortable (5) would you be with this system managing your medical data?

    *Very comfortable 1 2 3 4 5 Very uncomfortable*

52. How capable (1) or incapable (5) do you consider this system in handling medical data securely?

    *Very capable 1 2 3 4 5 Very incapable*

53. Please rate your agreement with the following statement: "I trust this system to handle my medical data **from my native country** in a safe and secure manner"

    *Strongly disagree 1 2 3 4 5 Strongly agree*

54. Please rate your agreement with the following statement: "I trust this system to handle my medical data **from other countries in Europe** in a safe and secure manner

    *Strongly disagree 1 2 3 4 5 Strongly agree*

## Perceived Usefulness Questions (PU)

55. Using the SERUMS technology would make it possible to share and get insight in my medical data across Europe

    *Strongly disagree 1 2 3 4 5 Strongly agree*

56. Using the SERUMS technology would make finding and sharing my medical information across Europe more efficient

    *Strongly disagree 1 2 3 4 5 Strongly agree*

57. Using the SERUMS technology would enhance my ability to retrieve and share my medical files across Europe

    *Strongly disagree 1 2 3 4 5 Strongly agree*

58. I would find the SERUMS technology useful

    *Strongly disagree 1 2 3 4 5 Strongly agree*

## Perceived Ease of Use Questions (PEU)

59. Learning to operate the SERUMS technology would be easy for me

    *Strongly disagree 1 2 3 4 5 Strongly agree*

60. I would find it easy to get the SERUMS technology to do what I want it to do

    *Strongly disagree 1 2 3 4 5 Strongly agree*

61. It would be easy for me to become skilful in the use of the SERUMS technology

    *Strongly disagree 1 2 3 4 5 Strongly agree*

62. I would find the SERUMS technology easy to use

    *Strongly disagree 1 2 3 4 5 Strongly agree*

## Behavioural Intention to use (BI)

63. I would intend to use the SERUMS technology when I need access to my medical files from my **native country**

    *Strongly disagree 1 2 3 4 5 Strongly agree*

64. I would intend to use the SERUMS technology when I need access to my medical files from hospitals **across Europe**

    *Strongly disagree 1 2 3 4 5 Strongly agree*

## Data ownership

65. I believe my personal information from my **native country** is accessible only to those authorised to have access.

    *Strongly disagree 1 2 3 4 5 Strongly agree*

66. I believe my personal information from hospitals **across Europe** is accessible only to those authorised to have access.

    *Strongly disagree 1 2 3 4 5 Strongly agree*

67. It is clear what information about me SERUMS keeps in the system.

    *Strongly disagree 1 2 3 4 5 Strongly agree*

68. It is clear who is the audience of my shared information.

    *Strongly disagree 1 2 3 4 5 Strongly agree*

69. I think SERUMS allows me to restrict the access to some of my personal information to some people.

    *Strongly disagree 1 2 3 4 5 Strongly agree*

70. I think I have control over what personal information I can share via SERUMS.

*Strongly disagree 1 2 3 4 5 Strongly agree*

71. It is clear what information about me caregivers from my **native country** can see on SERUMS.

*Strongly disagree 1 2 3 4 5 Strongly agree*

72. It is clear what information about me caregivers **across Europe** can see on SERUMS.

*Strongly disagree 1 2 3 4 5 Strongly agree*

## Perceived security of SERUMS system

73. Overall, how secure do you find the SERUMS system?

*Very insecure 1 2 3 4 5 Very secure*

74. I am not worried about the security of the SERUMS system

*Strongly disagree 1 2 3 4 5 Strongly agree*

75. I trust in the ability of the SERUMS system to protect my privacy

*Strongly disagree 1 2 3 4 5 Strongly agree*

76. I trust in the technology the SERUMS system is using

*Strongly disagree 1 2 3 4 5 Strongly agree*

# Appendix 4 - questionnaire for professionals

## General Background

1. What is your Age range (in years)?

   *18-25; 26-35; 36-45; 46-55; 56-65; 66 and above*

2. What is your highest degree of education?

   *Ph.D. Studies; Master Studies; Bachelor Studies; High School; Primary School*

3. What is your occupation?

   *Doctor; Nurse; Caregiver; IT Expert; Security Expert; Other*

4. How would you rate your computer literacy?

   *Beginner 1 2 3 4 5 Advanced*

5. Do you currently have regular access to a computer?

   *Yes, No*

## General Preference and Opinion about FlexPass

*Please explain your overall preference and opinions with regards to the FlexPass password system*

6. Do you like the idea of creating picture passwords with personalised images tailored to the users' prior daily life activities and experiences?

   *Not at all 1 2 3 4 5 Extremely*

7. Do you like the idea of allowing users to flexibly choose their preferred authentication method (picture or text password)?

   *Not at all 1 2 3 4 5 Extremely*

8. Do you believe that FlexPass would be a good alternative authentication method for patients?

   *Not at all 1 2 3 4 5 Extremely*

9. What are the positive aspects you like in the FlexPass password system?

   *Text field*

10. What are the negative aspects you do not like in the FlexPass password system?

    *Text field*

11. Would you be willing to use the FlexPass password system as an alternative user authentication system to login to your user account?

    *Yes, No*

12. Explain the reasoning behind your answer in the previous question

    *Text field*

## Password Creation

*Please rate your perceptions with regards to the FlexPass password creation system and process*

13. Overall, how difficult or easy do you find the password creation task in FlexPass?

    *Very difficult 1 2 3 4 5 Very easy*

14. Overall, how slow or fast do you find the password creation task in FlexPass?

    *Slow 1 2 3 4 5 Fast*

15. Overall, how secure do you find the FlexPass password system?

    *Very insecure 1 2 3 4 5 Very secure*

16. How strong do you believe a FlexPass password is?

    *Very weak 1 2 3 4 5 Very strong*

## Password Login

*Please rate your perceptions with regards to the FlexPass login system*

17. Overall, how difficult or easy do you find the login task in FlexPass?

    *Very difficult 1 2 3 4 5 Very easy*

18. How mentally demanding do you believe the login task is?

    *Very low 1 2 3 4 5 Very high*

19. Patients will easily log on to the FlexPass password system

    *Strongly disagree 1 2 3 4 5 Strongly agree*

20. Patients will effectively remember their password

    *Strongly disagree 1 2 3 4 5 Strongly agree*

## Two-factor Authentication Mobile Application

*Please rate your perceptions with regards to the two-factor authentication system*

21. Overall, how difficult or easy do you find the installation and enrolment to the two-factor authentication mobile application?

    *Very difficult 1 2 3 4 5 Very easy*

22. Overall, how difficult or easy do you find the two-factor authentication approval task (push notification)?

    *Very difficult 1 2 3 4 5 Very easy*

23. Overall, how secure do you find the two-factor authentication mobile application?

    *Very insecure 1 2 3 4 5 Very secure*

## Password Reset

*Please rate your perceptions with regards to the FlexPass password reset system and process*

24. Overall, how difficult or easy do you find the password reset process of the FlexPass system?

    *Very difficult 1 2 3 4 5 Very easy*

25. Overall, how secure do you find the password reset process of the FlexPass system?

    *Very insecure 1 2 3 4 5 Very secure*

## Trust

*Please rate your trust towards the FlexPass password system*

26. I trust in the technology the FlexPass password system is using

    *Strongly disagree 1 2 3 4 5 Strongly agree*

27. I trust in the ability of the FlexPass password system to protect the patients' privacy

    *Strongly disagree 1 2 3 4 5 Strongly agree*

28. I am not worried about the security of the FlexPass password system

    *Strongly disagree 1 2 3 4 5 Strongly agree*

29. I trust the FlexPass password system to protect my account and data from cybercriminals

    *Strongly disagree 1 2 3 4 5 Strongly agree*

30. Do you believe that FlexPass' personalised picture passwords would potentially reveal private information of users and raise privacy concerns?

    *Strongly disagree 1 2 3 4 5 Strongly agree*

31. In case you believe that FlexPass entails privacy issues, please elaborate on these and provide preferred methods to assure privacy-preservation. (optional)

    *Text field*

## Patient trust medical data

32. How comfortable (1) or uncomfortable (5) would you be with this system managing the patient's medical data?

    *Very comfortable 1 2 3 4 5 Very uncomfortable*

33. How capable (1) or incapable (5) do you consider this system in handling medical data securely?

    *Very capable 1 2 3 4 5 Very incapable*

34. Please rate your agreement with the following statement: "I trust this system to handle medical data in a safe and secure manner"

    *Strongly disagree 1 2 3 4 5 Strongly agree*

## Perceived Usefulness Questions (PU)

35. Using the SERUMS technology would make it possible to share and get insight in the patient's medical data

    *Strongly disagree 1 2 3 4 5 Strongly agree*

36. Using the SERUMS technology would make finding and sharing the patient's medical information more efficient

    *Strongly disagree 1 2 3 4 5 Strongly agree*

37. Using the SERUMS technology would enhance my ability to retrieve and share all patient's medical files

    *Strongly disagree 1 2 3 4 5 Strongly agree*

38. I would find the SERUMS technology useful

    *Strongly disagree 1 2 3 4 5 Strongly agree*

## Perceived Ease of Use Questions (PEU)

39. Learning to operate the SERUMS technology would be easy for me

    *Strongly disagree 1 2 3 4 5 Strongly agree*

40. I would find it easy to get the SERUMS technology to do what I want it to do

    *Strongly disagree 1 2 3 4 5 Strongly agree*

41. It would be easy for me to become skilful in the use of the SERUMS technology

    *Strongly disagree 1 2 3 4 5 Strongly agree*

42. I would find the SERUMS technology easy to use

    *Strongly disagree 1 2 3 4 5 Strongly agree*

## Behavioural Intention to use (BI)

43. I would intend to use the SERUMS technology when I need access to all patients medical files

    *Strongly disagree 1 2 3 4 5 Strongly agree*

## Data ownership

44. I believe the patient's personal medical information is accessible only to those authorised to have access.

    *Strongly disagree 1 2 3 4 5 Strongly agree*

45. It is clear what information about the patient SERUMS keeps in the system.

    *Strongly disagree 1 2 3 4 5 Strongly agree*

46. It is clear who is the audience of the patient’s shared information.

*Strongly disagree 1 2 3 4 5 Strongly agree*

47. I think SERUMS allows the patient to restrict the access to some of his personal information to some people.

*Strongly disagree 1 2 3 4 5 Strongly agree*

48. I think the patient has control over what personal information he or she can share via SERUMS.

*Strongly disagree 1 2 3 4 5 Strongly agree*

49. It is clear what patient information caregivers can see on SERUMS.

*Strongly disagree 1 2 3 4 5 Strongly agree*

## Perceived security of SERUMS system

50. Overall, how secure do you find the SERUMS system?

*Very insecure 1 2 3 4 5 Very secure*

51. I am not worried about the security of the SERUMS system

*Strongly disagree 1 2 3 4 5 Strongly agree*

52. I trust in the ability of the SERUMS system to protect my privacy

*Strongly disagree 1 2 3 4 5 Strongly agree*

53. I trust in the technology the SERUMS system is using

*Strongly disagree 1 2 3 4 5 Strongly agree*