mHealthcare Platform

TECHNICAL DESCRIPTION

March 2019

Socioemprende S.L.
José Faus 17
46023 Valencia
CIF.-B-98.997.075
1.- Corporate commitment

• The fundamental right to data protection allows the control and management of someone’s personal data, enabling them to know at any time who handles it, as well as its destination. This right is regulated by Organic Law 15/1999, December 13 for the Protection of Personal Data, and Royal Decree 1720/2007, December 21 which unfolds it, whose purpose seeks to guarantee and protect, in terms of personal data’s treatment, public freedom and fundamental rights of natural persons and, especially, their personal and family privacy and honor.

• The Management of SOCIOEMPRENDE SL guarantees the privacy, adequacy, relevance, accuracy and updating of the personal data it manages, as a consequence of the provision of security services, in accordance with legal requirements. To this end, the levels of protection legally required have been adopted and technically, measures that have been implemented to prevent loss, misuse, alteration or unauthorized access.

• The personal data processed is incorporated into files duly registered with the Agency for the Protection of Personal Data, and in no case they are used for purposes other than those authorized by the owner thereof. Likewise, they will not be transferred to third parties without the express consent of the owner, in which case they will be informed specifically about their purpose and the identity of the assignees.

• The holders of personal data are recognized and may exercise the rights of access, rectification, cancellation and opposition to the processing, use and transfer of their data by written communication and sent to the postal address of the responsible organization. All these issues, as well as the measures established to ensure the protection of personal data, are set out in detail in this Security Document.

• The management of personal data of users by SOCIOEMPRENDE SL as well as the sending of commercial communications made by electronic means are respectively consistent with the general regulations in force: Organic Law 15/1999, December 13, Protection of Personal Data and Law 34/2002, July 11, Services of the Information Society and Electronic Commerce.
1.1.- About the regulatory changes of May 2018 in SPAIN

• Socioemprende SL has carried out the following actions to adapt itself to the new data protection regulations and can prove it:
  • It has created a record of treatment activities.
  • It has reviewed and updated the legal notice of the web and the application.
  • It has reviewed and updated that the interested party is offered the information according to art. 14 of the RGPD prior to obtaining consent.
  • It has reviewed the process of obtaining the explicit and unambiguous consent of each user of the mHealthCare Platform.
  • All employees of SOCIOEMPRENDE SL have received training on personal data protection and have signed confidentiality agreements with all the information required by the RGPD.
  • All the external services of SOCIOEMPRENDE SL that have access to the application’s data have been reviewed to confirm that they comply with the regulations on data protection and have signed a Confidentiality contract.
  • A Delegate for Data Protection has been appointed, this appointment has been communicated to the Spanish Agency for Data Protection. A contract has also been signed with the DPO with its obligations and is already in effect.
  • Taking into account the state of the art, the costs of application, and the nature, scope, context and purposes of treatment, as well as the risks of variable probability and severity for the rights and freedoms of natural persons, there have been applied appropriate technical and organizational measures to guarantee the level of security appropriate for the risk (following the recommendations of article 32 of the RGPD).
  • Before making any change that may affect data processing, SOCIOEMPRENDE SL has established a protocol to evaluate its possible risks and determine the need to carry out an impact assessment prior to the start of said changes.
  • A protocol has been created to detect and report security breaches within 72 hours, as well as an action plan to mitigate or reduce its possible consequences, there is a registry of incidents that is reviewed periodically to evaluate the corrective measures.
  • Protocols have been created to manage requests for rights: ARCO (access, rectification, cancellation and opposition), portability, limitation of treatment and the right not to be subject to automated decisions.

1.2.- About the files hosted in the patient folders

• The personal data of the patients registered in the Platform of SOCIOEMPRENDE SL is property of the Patients. At the time of registration, the patient accepts that their personal data will be hosted by SOCIOEMPRENDE SL and will be accessible by a closed list of previously authorized professionals, including technical call center personnel of SOCIOEMPRENDE SL, who will have access to see or treat that data.

• However, the data that the medical and pharmaceutical professionals introduce in the personal folders of the patients hosted by SOCIOEMPRENDE SL, in addition to those data that could be automatically integrated with the information systems of the Hospital or the health ministries, are clinical data whose responsibility for the treatment is the Hospital Center and not SOCIOEMPRENDE SL. In this scenario, therefore, a contract for the processing of data by third parties between the Manager (Hospital) and the Supervisor (SOCIOEMPRENDE SL) is required to ensure compliance with the requirements and responsibilities of the legal framework to deal with the transfer to third parties of those data.

• Regarding the physical location of these DATA, whether personal data or clinical data, IT IS NOT STRICTLY NECESSARY TO BE ACCOMMODATED WITHIN THE INFRASTRUCTURES OF THE HOSPITAL. However, in the event that they are not, the Data Manager must ensure that the Treatment Supervisor -who is hosting them- abides by, not only the legal and consent measures, but also a series of rules regarding physical, logical and corporate security policies.
1. Corporate Commitment (cont.-)

- Fundamentally, SOCIOEMPRENDE SL has the following:
  - All infrastructures, servers and databases have data encryption systems, source code encryption, secured access with keys and physical protection systems of the hosting environment.
  - The Cloud Architecture has a dedicated server that hosts the personal data of the users leaving the production and test machines operating in anonymous environments.
  - It incorporates certification of the Aenor quality standards required for the production of software in the certification of CE marking as a medical device of class I

1.3. Accommodation of images and multimedia files that users keep

- Special categories of data should be treated for health-related purposes when necessary to achieve those ends for the benefit of individuals and society as a whole.

- In the case of SOCIOEMPRENDE SL, also according to art. 9.2a of the EU Regulation 2016/679 (hereinafter RGPD), the treatment can be done because the interested party has given his explicit consent for the treatment of such personal data for the specified purposes.

- SOCIOEMPRENDE SL complies with the principles relating to the treatment- set out in art. 5.1 of the RGPD, because these data collected are treated in a lawful, loyal and transparent manner, always informing the interested party of all the aspects included in art. 14 of the RGPD; the data is collected for specific, explicit and legitimate purposes and is never treated in a manner incompatible with those purposes.

- The data is always adequate, relevant and limited to what is necessary in relation to the purposes for which they are treated, SOCIOEMPRENDE SL always applies the principle of data minimization. Any time, reasonable measures are taken so that these data are rectified or deleted without undue delay, when they are inaccurate for the purposes for which they are treated.

- The data are maintained in such a way as to allow the identification of the interested party for no longer than necessary for the purposes of the treatment and are treated in such a way as to ensure adequate security, including protection against unauthorized or illegal treatment, their loss, destruction or accidental damage, through the application of appropriate technical and organizational measures. In addition SOCIOEMPRENDE SL can demonstrate all these extremes.

- In conclusion SOCIOEMPRENDE SL has legitimacy to perform this type of treatment because the interested party has given his consent, is applying the appropriate security measures and the data SOCIOEMPRENDE SL collects are appropriate to the purposes of the previous information that has been provided to the interested party, they are accurate and they are necessary for these purposes.
2. - Architecture

The following chart shows the server and access diagram of the mHealthcare Platform of SOCIOEMPRENDE SL.

- **Patient Access to the Platform:**
  - It is usually done from mobile phones with IOS and Android operating systems, although users also have a Web PC access from conventional browsers such as Google Chrome, Internet Explorer, Safari, etc.
  - Patient access requires a username and password.

- **Professional Access to the Platform**
  - It is usually done from personal computers located in hospital consultations and administration and management positions. The front end of the professional access is optimized for google-Chrome web browser, although access is also allowed from other conventional browsers. The current graphical and traffic light load prevents professional access from the phone.

- **CLOUD Servers that host the Platform (CORE):**
  - **PRODUCTION Server**
    - Currently, the core platform only uses the production server and the patient databases that it contains. The Production Server also has external links to the contents of the "Education Server" and links to the "BI Server" for integrated applications with third parties (Hospital HIS). Additionally, it communicates with the AEMPS web service to obtain the update of the new medicines.
  - **PRE-PRODUCTION server**
    - The preproduction Server is a copy identical to the PRODUCTION one, with the difference of having all patient data totally obfuscated or confused. This server is against which the development team tests the new versions before making the deployments in production.
  - **EDUCATION Server**
    - This machine contains educational contents and recommendations to the user that are structured by pathologies and by projects. Depending on the target of the project, the user is taken to the sections of the database that correspond to their health problem or their care plan.
  - **PATIENT Server**
    - This machine has been contracted to locate the personal data and multimedia files of the patients in order to have them separated from the rest of the infrastructures. Throughout 2019 the patient files of each project will be migrated to this server.
Video Conferencing Servers - SIGNALING / TURN

- Signaling (WSS Server): Software element that is responsible for "signaling" the communication between the actors (room management, codecs accepted, input and output of actors ...)
- Nateo (Server TURN / STUN): Software element that acts as an intermediary of the streams (video, audio and data) when some actor (or both) can not establish it directly.
3.- Logical Model

• The application consists of a set of REST services published on the internet, which consume the Android app, the iOS app and the web, both professional and patient use. The REST services communicate with the different applications through GET and POST methods, receiving and sending JSON objects. Currently (November 2018), there are two types of user authentication, depending on whether the request is made from a web browser, or directly from one of the app's:

1.- Browser Authentication:
• The user (whether patient or professional) is authenticated by user and password in the login form of the web. If the data is correct, the system creates a valid access token for only 60 minutes. A session object is created on the system with this token, and it is returned to the client through a cookie. Once 60 minutes pass (or there is no cookie in the browser), the system automatically redirects to the login screen.

2.- Authentication App:
• The user (patient only) is identified by the login screen when opening the app. The system validates user and password, and if they are correct, generates an access token that is returned to the app along with the data of its user.

• From this moment, all the requests that the app makes to the system, such as recording drug shots, registering progressives, etc., must go with this access token.
  • If the token is correct and is not expired, the system will process the request. If the token is not correct, or it is expired, the system will obtain the user's data.
  • If the user is correct, it is active, and the password has not changed, it is "relogged" generating another valid access token.
  • If any of the data is not correct at the time of generating another token, it is directly returned to the user's login page.
4.- Functional Scope

1.- Actors

- **PATIENTS**
  - Once the professional creates and registers the patient on the platform, the system generates the access codes for the user and automates the consent process.
  - The patient can then access your application from a personal computer or from free native mobile applications available in Google and Apple stores (Android and IOS).

- **PROFESSIONALS**
  - The access of professionals to the platform is done from their computers through a web portal.
  - In addition to the patient's discharge into the system, they will be able to customize their care plan, establish diagnoses and risk factors, prescribe medication and non-pharmacological treatments, follow-up, etc. They have a powerful remote monitoring system based on alerts and semaphores linked to individual patient objectives.

- **TECHNICAL CALL CENTER**
  - Patients have a telematic support service to resolve incidents related to technology, phones or their use.
  - The staff of the call center of SOCIOEMPRENDE SL also supports the process of incorporating patients with online training in the applications’ management.
  - This same service provides educational support to professional personnel who join the project.

- **HOSPITALS**
  - In each Hospital, a data treatment contract is signed where the center acts as responsible for said treatment and agrees the contractual relationship with the provider, as the person in charge of the treatment.
  - In the Hospital Centers that so wish or allow, the Platform allows the integration of the data that come from the corporate information systems (demographic data, diagnosis, test results or pharmacological prescription, being able to be integrated bidirectionally).

- **The SPANISH DRUGS AGENCY**
  - The Ministry of Health, and in particular, the Agency for Medicines and Health Products (Spanish Agency of Medicines and Medical Devices), acts in the system as a provider of the drug database.
  - The Platform connects every night with the National Agency to update the drugs, their additions and deletions, and provides important information about each pharmaceutical product (dosage presentation, prospectus, photograph, etc.)
  - The drug database that resides in mobile device applications is periodically updated in a planned manner.

- **CLOUD SERVICES PROVIDER**
  - The platform is hosted in the cloud
  - The current provider of the infrastructures of the mHealthCare Platform of SOCIOEMPRENDE SL is the STRATO company and the CPD infrastructures are physically located in Germany.

- **MEDICAL OR WEARABLE DEVICES**
  - The platform is integrated with medical devices for measuring cardiovascular variables for automatic measurements of blood pressure or heart rate.
  - There are currently several devices integrated through Bluetooth® connectivity under the connectivity layers of Google Fit and Apple Health.
2.- Functional Map

(FUNCTIONAL LAYER AND CLOUD ARCHITECTURE)

- CLINICAL DATA
  - The clinical data module allows the specific design of the card of the patient with certain pathology.
  - The standard structure of this module includes standard blocks (Diagnoses, Allergies, antecedents, risk factors, etc.) and a fourth block with the baseline and evolutionary control variables specific to each disease or project.

- PERSONAL INFORMATION
  - The personal data module includes four data profiles:
    - Demographics of the patient,
    - Data of tutor or contact person -if applicable-,
    - Care and relationship data with the provider,
    - Professional contacts assigned
  - This last section allows activating and legalizing the access of professionals to the patient's data and their personal folder of Health

- SELF-CONTROL AND QUESTIONNAIRES
  - The care plan for each disease includes a list of modules or subprograms for self-monitoring by the patient. It integrates different bi-dimensions and control modules:
    - General condition, heart rate and blood pressure
    - Glycemia, Weight and perimeters
    - Relevant analytical data
    - Food, diet, exercise, training
    - Smoking and give smoking up cessation systems
  - It also includes validated questionnaires to guide patients according to the project (therapeutic adherence, quality of life, mood, etc.).
  - The platform currently has a library with more than 40 SELFCONTROLS and QUESTIONNAIRES configurable by project.

- TREATMENT
  - The Platform has a powerful prescription module, self-prescription by the patient, adherence control and therapeutic compliance.
  - It includes pharmacological treatments and other therapies.
  - It has optional subsystems that are loaded depending on the project, such as remote authorization before self-prescription by the patient.
  - Professional access also offers compliance indicators in graphical mode as the image shows.
2.- Functional Map

**PROFESSIONAL-PATIENT MESSAGING**
- The platform incorporates a bidirectional messaging system between professionals and patients.
- It is a simple interface to share messages and optionally include the sending of multimedia files.
- For the patient with his APP, automatic push messaging is used with message entry warnings.
- When important or critical notifications, the professional can verify remotely if the patient has read it.

**EDUCATION AND TIPS**
- The pedagogical health library "educahealth" incorporates the training contents of patient assistance.
- It is an external server that, as a content repository, integrates perfectly with the mobile applications of the platform.
- It allows to load in a structured way, under simple navigation menus, text files, images, videos or external links.
- It is a responsive portal that is embedded within the Apps.
- Professionals may have access permissions to educahealth publication manager to enrich the content library.

**PROFESSIONALS. MONITORING AND ALERTS**
- Health professionals (doctors, pharmacists, nurses ...) have an online access to the real state of their patients' behavior and have a powerful control and remote monitoring control panel.
- Functionally, the main services you can enjoy are:
  - Patient Registration and Automated Consent Process
  - Access to the individual folder of each patient
  - Prescribe a PLAN OF SELF CARE, Prescription of TREATMENTS
  - Control of status and risk by SEMÁFOROS
  - Criticality alerts via email and SMS, Patient Messaging (push App)
  - Patient cohort statistics
  - Data export systems

**PROFESSIONALS. TRAFFIC LIGHTS**
- The traffic lights of the Platform, represented by iconography, allow to quickly identify the status of a Patient's Self-Care Plan.
- Through colors associated with risk states, it allows management and prioritization of the actors responsible for remote monitoring based on risk criteria.
• SOCIOEMPRENSE SL has its own infrastructure hosted in third-party datacenter. The following describes the features of the CPD and of the entire infrastructure assigned to the project.

• SOCIOEMPRENSE SL uses the data centers of STRATO, which are listed among the safest in the world and are subject to the strictest controls to comply with the most stringent security standards in terms of data protection and security.

• This datacenter hosts the information of about four million web pages and more than 50,000 servers. All data is stored exclusively in the high security data centers in Germany and is protected by the German Data Protection Act, one of the strictest in the world.

• The CPD also has the TÜV seal according to ISO 27001 (previously 7799) since 2004. In essence, this badge proves an exceptional level in terms of availability and security of all services in data centers. In addition, this certification includes numerous security measures in the IT infrastructure itself, in secondary technology and in the process chain. The CPD has been certified annually since 2004, always according to ISO 27001.

• STRATO incorporates a strict security agreement that guarantees the maximum availability of the data and the best protection of the same.
  • Redundant data centers
  • Supply of uninterrupted light supported by batteries
  • Emergency supply for autonomous management of up to four weeks
  • Laser warning of fire and extinguishing agents
  • Confidential location of data centers

• STRATO is responsible for the physical security of its data centers but also for the customer's own data, providing them with various security functions such as:
  • Backup Manager, with which the most important data can be saved from the hard disk itself to the STRATO server.
  • Backup Control, which regularly creates backup copies of all data online and offers customers online access to them in up to 10 different backup versions.
  • SecurityScan, which detects open ports and security holes, and reports on them.

• The high performance equipment and the direct connection to the Internet neutral points ensure short load times and data traffic with optimal performance.
Platform Security (SSL)

- SOCIOEMPRENDE SL incorporates the SSL (Secure Socket Layer) certificate in its infrastructures, an Internet protocol that encrypts all the data of a transfer, which prevents third parties from gaining access to confidential data.

- The SSL certificate provides security to the visitor of the website that indicates that the site is authentic, real and reliable as to enter personal data.

- The security protocol allows the data to travel in an integral and secure way, that is, the transmission of data between a server and web user, and in feedback, is fully encrypted or encrypted. The data travels encrypted and for this mathematical algorithms and a system of keys are used that are only identified between the person who navigates and the server. By having a reliable SSL certificate the data is encrypted and nobody can read its contents.

- The servers create a path with a unique encryption for private sessions through Internet, the public key of the server is accessible and that is why we use a public key and a private key: the public key is to encrypt the information, the private key to decipher it.

Security in the Mobile Application (code encryption)

- Given the open source nature of mobile applications, especially Android ones, the use of obfuscation in the code is recommended as a minimum.

- The application protection implemented by SOCIOEMPRENDE SL incorporates protection techniques and several layers of defense to fully ensure the complete application. It has end-to-end security for native mobile applications, enabling the protection of code, data and cryptographic keys that reside inside and are part of the operating system applications where algorithms and sensitive data are stored.

- The security solution of SOCIOEMPRENDE SL provides automatic defense, with detection and reactive capabilities, through the deployment of various security techniques (called Guards) with obfuscation, checksum and anti-debug techniques that are directly applied in the software code of each application, to protect the binary code.

- The sum of the layered technology provided by SOCIOEMPRENDE SL for the protection of its Apps prevents passive and active analysis, as well as providing integrity in applications in such a way that it does not impact the source code, the functionality of the application or the development process.
6.- Security (cont.-)

Security in the Communication Channel

- SOCIOEMPRENDE SL offers guaranteed security with end-to-end secure connections with encryption of communication and use of international standards.
- The transmission of information is an essential factor that allows remote medical actions or tele-consultations, and to associate different types of communication files (text messaging, chats, audio, static images or video sessions), both among professionals (interconsultations) as in the doctor-patient relationship.
- The communication channel has a limited bandwidth, so it is important to compress and secure the information. For this, SOCIOEMPRENDE SL uses international standards of the sector (HL7) that allow the capture, transmission and reception of biomedical information.

- Regarding the securing of videoconferencing for virtual consultation sessions, the signals provided by the cameras, the microphone and peripheral equipment are sent to the CODEC (encoder-decoder) which performs a complex process in three stages:
  - The CODEC converts audio and video signals to a computer code (digitization process). The information is reduced in small packages of binary data (1 or 0). In this way data is transmitted requiring less space in the communication channel.
  - The data is sent to another communication device, which transmits them to the remote site through the transmission channel (ADSL, fiber, 4G ...) through which they will travel.
  - Through the transmission channel, the other site receives the data through the communication device which delivers it to the CODEC, in charge of decoding the audio and video signals and sends them to the monitors to be seen and heard by the people who attend the event.

Access Security (AAA).

- The AAA (Authentication, Authorization & Accounting) protocol is a security mechanism for user access.
  - Authentication. Process of trying to verify the digital identity of a communication sender as a request to connect, a way to ensure that users are who they say they are.
  - Authorization. Process by which the database authorizes the identified user to access certain resources of the same.
  - Audit. Through which the network or associated systems record each and every one of the accesses to the resources that the user makes, authorized or not.
- The authentication methods implemented are based on two keys, user and password, which make it a reliable, accessible and acceptable system for users.
Password expiration policy

- The initial logic model implemented in the mHealthCare platform required the user to change the password every 6 months.
- After the experience of several years with patients in self-control regime, and taking into account the security risks for accessing to daily medication that caused the automatic expiration of the keys, it was decided to implement a six-month automatic notice model in the summer of 2018 with the recommendation of password change.
- This new system, however, does force users to modify their password after 18 months of using the last modified password.

Database Audit. Access to the Patient Health Folder.

- The mHealthCare platform of SOCIOEMPRENDE SL allows obtaining audit reports on demand from clients (Hospitals).
- This process allows to measure, ensure, demonstrate, monitor and record the access to the information stored in the databases.
- The reports allow you to determine which user has accessed what data and what type of activity it has performed on that data between dates.
- Regarding the power of a patient to request who has seen their clinical data, who has prescribed a medication or has prescribed a biomedical control, for example, the Platform has an internal audit on demand to respond to this request.
- The requests must be delivered to SOCIOEMPRENDE SL in writing, signed by the Head of Data Processing (hospital center) and accompanied by the express request of the patient or user who requests it.

- The ANNEX to this report presents the new security measures foreseen by SOCIOEMPRENDE SL for its execution in the first quarter of 2019.
7.- Quality. Medical Device

- The Platform records-registers the evolution of the patient's disease in terms of symptoms, adverse effects, constants and adherence to medication.
- At the moment in which the application orients the patient or the doctor showing an alert or another in place of the recorded symptomatology, it becomes a medical device (Class 1) and requires compliance with the conditions stipulated by current legislation to show the CE mark.

(Quality measures and processes required (regulations))

- Currently, our Quality Management System monitors compliance with the corresponding harmonized standards required:
  - Quality management system according to the sanitary scope ISO 13.485
  - Management of the IEC 62304 software life cycle
  - Risk management ISO 14.971
  - Clinical evaluation
  - Post-marketing monitoring.
  - Protection of personal data: LOPD 15/1999, RDL 13/2012, Regulation EU 2016/679 (RGPD)

Contents Clinical validation

- Among the documentation to be collected when the functional analysis of our application and its adaptation to each pathology is carried out, advice and recommendations specific to the pathology are collected, which the clinical staff must adequately reference.
- In addition, the ranges of values that are defined to support decision-making or recommendations in a notice format to be displayed to users are adequately documented by associations and / or clinical publications, with physicians responsible for filling in scientific corresponding references.

Class II Medical Device.

- Currently (March 19) SOCIOEMPRENDE SL is in the phase 2 development of a multicenter research project on 12 hospitals for patients’ monitoring and self-control with inflammatory bowel disease that will allow to initiate the procedures -to apply to the AEMPS\textsuperscript{1} of the platform’s Class of Marking CE allowing its evolution from Class IIa to Class IIb.

\textsuperscript{1}-AEMPS. Agencia Española de Medicamentos y Productos Sanitarios. Ministerio de Sanidad