RemindMeCare (ReMe.care) Information Security

Document detail:

Company Name	**Health-Connected Ltd**
Completed By	**Etienne Abrahams**
Job Title	**Director**
Completion Date	**26/05/2017**
Version number	**1.8**

THIS DOCUMENT AND THE INFORMATION IN IT ARE PROVIDED IN CONFIDENCE AND MAY NOT BE DISCLOSED TO ANY THIRD PARTY OR USED FOR ANY OTHER PURPOSE WITHOUT THE EXPRESS WRITTEN PERMISSION OF HEALTH-CONNECTED Ltd.

Table of Contents

1. System Users

1.1 User types

RemindMeCare (ReMe.care) supports the creation and administration of 6 specific user types:

a. Informal carer: Friend or family member
b. Formal carer: Professional staff member
c. Exclusive Formal Carer: Staff member who can selected service user records
d. Formal Carer Admin: Administrator of Formal carers for one organisation
e. Person with dementia: Service user who ultimately owns the information in their Profile
f. Primary carer: Formal or Informal carer with similar access rights to the person with dementia
g. Family admin: Similar rights to the Person with dementia

1.2 User Privileges

1.2.1 Informal Carer

Invited via email by the person with dementia, a formal or other informal carer. This user role enjoys basic privileges available to all other users. They can:

a) Access a single person with dementia's Profile and Care Circle
b) Create any Topic in the user's Profile
c) View, Edit and Delete any Topic in the user's Profile that has unrestricted access
d) Upload photographs to any Topic in the user's Profile that has unrestricted access
e) Write a note and Read all existing notes
f) Create and Delete one to one Sessions
g) Review a Session that they have been invited to
h) Send a message requesting a new informal carer is invited to join the user's Care Circle

1.2.2 Formal Carer

Invited via email by the Formal Carer Admin for their care organisation. They have the same rights as an informal carer, but they can also:

a) Access the Profile of any service user associated with their organisation.
b) Enroll new service users
c) Create Group sessions with all participants from their organization

1.2.3 Exclusive Formal Carer

Same rights as the Formal Carer, but only has access to a subset of the Organisation's service users. The list of individuals that can be accessed is defined by the Formal Carer Admin.

1.2.4 Formal Care Admin

This formal carer role has administrator rights over their colleagues. When a new care organisation is enrolled a Formal Carer Admin is also created. In addition to their formal care colleagues, this user can:

a) Invite formal care colleagues to join their organisation
b) Activate and Deactivate the accounts of their colleagues
c) Transfer the role of formal carers within their organisation

1.2.5 Person with Dementia

Enrolled by a Formal carer or the Organisation's Formal Carer Admin. This user can:

a) Activate and Deactivate the accounts of Informal carers
b) Invite new informal carers
c) Invite a new care organisation to access their Profile
d) Make any individual profile Topic private by identifying those users that should be allowed access.
e) Can undelete any profile Topic or Session summary that another user has chosen to remove

1.2.6 Primary Carer

Same rights as the Person with Dementia. The role is initially given to the Local Carer Admin of the organisation that enrolled the person with dementia. The role can be transferred by the Primary carer themselves, to any formal or informal carer within the service user's care circle. This user has the same privileges as the person with dementia themselves. In addition, they can:

a) Transfer their Primary carer role to any informal or formal carer within the person with dementia's invited care circle.

1.2.7 Family Admin

Same rights as the Person with Dementia. This role is automatically given to the first Informal Carer invited. A single user can hold the Primary Carer and Family Admin roles simultaneously and these can be transferred separately.

2. Data capture:

2.1 Account creation

To create an account, formal and informal carers provide:

Name
Preferred name
Gender
Relationship to the person with dementia
Unique email address
Unique username
Unique Password

In addition, to enroll a person with dementia we collect:

Ethnicity
Mother tongue
Year of Birth (not full date of birth)
Rating of hearing and vision
Personal email address (if available)
Email address of a family member

Copies of the person with dementia's credentials are sent to the Family Admin and where appropriate the Formal Carer Admin.

2.2 Enrolment and consent

2.2.1 Family registration

In order to enroll a new service user, a system generated invitation email is sent directly to the email account of a family member or friend. The recipient follows a link in the email to a form where they enter enrolment details for the new service user. These details include the email address of a family representative who is automatically registered as the family administrator for the account.

2.2.2 Formal care registration

A senior carer within the organisation can enroll service users without family involvement. This is an exceptional step taken when no family or friend is available to complete the enrolment process. The first informal carer to register is subsequently appointed family administrator.

A record of the registration type is recorded as part of the service user's account information.

2.3 Data captured during system use

2.3.1 Person identifiable data

Overview: The system constructs a profile of the person with dementia. The profile is built up of Topics of interest to the individual. Each Topic consists of a set of keywords known as a Nugget as well as links to 'favourite' content. Nuggets are used to perform a safe search of the web for individual pieces of content in the form of images and music. The person with dementia's responses to these individual pieces of content are recorded to refine the interests and preferences stored in the user's profile.

The system captures changes to these keywords, alongside notes, and content flagged as 'favourite' or 'unsettling'. Themed Topics include the definition of cultural information such as faith, work, places and events of importance

a) Topics can be restricted to enable access only to specific users
b) No information relating to financial details including address is stored
c) No information relating to medical records is stored
d) A record of the logged in carer and person with dementia is stored for each session.

2.3.2 Information Commissioner's Office

This enhanced "Quantified self" information is managed under the full DPA Regulations. To ensure compliance with these principles we have registered Health-Connected Ltd and ReMe.care with the Information Commissioner's Office reg. ZA 093002 and have appointed Etienne Abrahams to lead our work on ensuring compliance with the Data Protection legislation, our commitment to the principles of freedom of information and to meeting our high standards of operation of ReMe.care

3 Logical access security to web interface/system/application:

3.1 Account and password policies

Each user is provided with a unique ID. Password minimum length is 4 alpha numeric characters. Account lockout occurs after 5 failed attempts to login. The user's Family admin and Formal Carer Admin are emailed to alert them of the failed login attempt or request for password change.

3.2 Duration of active session

By default a session stays active for 12 minutes, after which time credentials must be re-entered.

3.3 Control and administration of permissions

An employee within the care organisation is assigned Formal Carer Admin status and has control of the permissions for your staff and service users.

3.4 Audit logging

Activity is logged across the tiers of the application in order to detect suspicious activity. Data will be collated on successful and unsuccessful logon attempts and changes to carer permissions.

Changes to a client's profile information and all users' biographies and notes will be both collated independently and displayed to users within the application.

4 Web interface/ system/application

4.1 Security protocol for the web interface / system/ application

The HTTPS communications protocol is used for secure communication over the Internet. AES is used to encrypt database fields.

4.2 Browsers compatibility

Initially, we fully support the latest versions of the Chrome browser (Mac, Windows, iOS and Android)

The front-end application will be compatible with the following browsers:

Safari (Mac and iOS only)

Firefox (Mac, Windows)

Opera (Mac, Windows)

We will support versions 9, 10, 11 of Internet Explorer on the Windows operating system.

4.3 Data upload / download: Security protocol used and encryption level

All management systems including data upload and download are only accessible via a VPN.

Personal content is uploaded by logged in users with SFTP over TLS.

In addition to ISP controls, all searches for content with ReMe are subject to the Microsoft Bing Search API's 'Strict safe search' feature to filter explicit results.

4.4 Port(s) on client's Firewall

It is not envisaged that any access to servers operated by the client will be required. Our application uses standard web ports

4.5 Changes needed to be made to client's firewall to allow the application to work

If the customer operates one, the white list for authorized web access from residential care facilities should include URL for ReMe.care itself and YouTube. ReMe.care will work without further changes to website access rules, but users may fail to access material if they choose to follow external links that we make available for legal attribution purposes. We are happy to work with the customer's security team in defining this.

5 Disaster recovery, back up and failover:

5.1 Data Centre(s)

Our application, ReMe.care is hosted with Softlayer an IBM owned company. Physically the servers are housed at their datacenter in London, a tier 3 data center with heightened security: electric fence around the whole building, biometrical identity check and 24/7/365 security surveillance.

5.2 Disaster Recovery /business continuity plans

The application is hosted in London at the IBM Softlayer. The site's Information Security Management and Business Continuity Systems are certified for ISO 27001 and ISO27017

5.3 Back-up procedure

All virtual machines are backed-up daily during night time. Data will be saved for a minimum of 30 days and a maximum of 365 days.

Full vm restores as well as file level restores are supported.

Offsite backups are available upon request.

5.4 Failover arrangements

Network, computing and power are fully redundant, both on the datacenter level as on the Softlayer infrastructure level.

6 Security of data and databases:

6.1 Physical location of hosted data

Our hosting agreement stipulates a server that is dedicated to Health-Connected's ReMe.care application The application is hosted in London at the IBM Softlayer's datacenter. The site's Information Security Management and Business Continuity Systems are certified for ISO 27001 and ISO27017

6.2 Company compliance

IBM Softlayer comply with the privacy and data protection laws outlined here see http://www.softlayer.com/compliANCE.. Certification available on request.

Health Connected have prepared a submission to the Information Commissioner's Office reg. ZA 093002.

We are aware of and will comply with the forthcoming European GDPR including mandatory disclosure of breaches. Evidence of Specific informed consent at a patient level is difficult due to the nature of the data subject's illness and falls in the scope of the clinician. Our application, ReMe.care offers facilities to record such approval has been sought.

6.3 Number of data breaches in the last 12 months

Our application, ReMe.care and its supporting Data have not suffered any Data Breaches. Should they occur we will disclose them according to our legal obligations.

6.4 Logical access controls to the database

Login is achieved with private keys over SSL. MySQL database fields contain AES (256) encrypted data.

Data shared between the server and web browser relies on the SSL protocol. On the database, AES or Advanced Encryption Standard 256 bit encryption is employed.

In terms of controls to limit users' access, the presence of a client's information on the ReMe.care system is only evident to a registered user if they have been explicitly invited to access the client's profile. This access is granted by invitation from an existing registered user. Users with Formal Carer Admin permissions and above receive notifications of all invitations issued.

In order to accept an invitation a user must register or enter existing credentials.

Formal and informal carers have access to read and write profile information in all areas except those topics defined as private or sensitive by the client, their Formal Carer Admin, Family Admin or Primary Carer. All changes to a profile are attributed to the logged in user and a record of these is presented within the ReMe.care package.

The Primary Carer, Family Admin and Formal care admin have ultimate control over access rights.

6.5 Account credentials protection within the database

User credentials are hashed as sha1 with a strong salt.

6.6 IT incident management procedure

All servers managed by IBM Softlayer are being monitored 24/7/365, including security monitoring. Incidents and alerts are escalated to their engineers and Health-Connected's staff via a set of communication tools.

While IBM Softlayer provides infrastructure (e.g. storage, computer power), Health Connected are ultimately responsible for the storage and processing of all client data.

6.7 Process for returning customer data when a request is received

Customer data is stored for a minimum of 30 days. IBM Softlayer provide secure tools and procedure for restoring data and downloading to transferable physical media. All management systems including data upload and download are available to Health-Connected and accessible via a VPN. Data would be downloaded and made available after written request from the customer

7 Operational and network protection including web portal:

7.1 Antivirus / malware / spyware protection

IBM Softlayer monitoring system detects suspicious behavior and abuse. Hacked websites will be disabled immediately, unless otherwise agreed. Health-Connected Ltd will receive automated alerts when abuse occurs and will always contact the customers impacted.

Rulesets are updated regularly

7.2 Firewalls in place

Hardware firewalls are implemented on both the router and server level. On the router level, basic DDoS protection is in place. In addition software firewalls are configured on the server level.

7.3 Patch management process

Patch management is scheduled on a regular basis. The exact timing for standard server configurations, is decided for by IBM Softlayer. For custom configurations like ReMe.care, patching is done in agreement with the customer.