

 E-Care @ Home

**WP1: User Requirement and Specification**

**D1.3: Specification of the IT architecture**

|  |  |
| --- | --- |
| Deliverable id | D1.3 |
| Document name | Specification of the IT architecture |
| Date | 15.10.2013 |

|  |
| --- |
| COVER AND CONTROL PAGE OF DOCUMENT |
| Project number: | 600451  |
| Project name: | E Care@Home  |
| Document id: | D1.3 |
| Document name: | Specification of the IT architecture |
| Dissemination level\* | Private |
| Version: | 1.0 |
| Date: | 15.10.2013 |
| Author(s): | Hospital Organiser AS, Valentin Garkavy |

|  |
| --- |
| ABSTRACT |
| Specification of the IT architecture, covering smartphones, tablets and servers infrastructure |
| KEYWORDS |
|  |
| VER. | DATE | STATUS, CHANGES | FROM | REVIEW |
| 1.0 | 15.10.2013 | First draft  | HOAS |  |
| 1.1 | 30.12.2013 | Ready for review version | HOAS |  |
|  |  |  |  |  |
|  |  |  |  |  |

Contents

[Preface 5](#_Toc376965617)

[Disclaimer on assumptions and limitations 5](#_Toc376965618)

[Solution architecture 6](#_Toc376965619)

[Solution components requirements 6](#_Toc376965620)

[System deployment scenarios 6](#_Toc376965621)

[HomePad 7](#_Toc376965622)

[HomePad General Hardware requirements: 7](#_Toc376965623)

[HomePad general software requirements 8](#_Toc376965624)

[HomePad software integration requirements 9](#_Toc376965625)

[Health and wellness sensors 12](#_Toc376965626)

[Central Management Portal (further - CMP) 12](#_Toc376965627)

[Central Management Portal Hardware minimal requirements 13](#_Toc376965628)

[Central Management Portal Software minimal requirements 13](#_Toc376965629)

[Friends and Family portal and Informal Care portal (further - FFP) 13](#_Toc376965630)

[Smartphone Portal (v2) (further - SP) 13](#_Toc376965631)

[Smartphone Portal Hardware minimal requirements 14](#_Toc376965632)

[Smartphone Portal Software minimal requirements 14](#_Toc376965633)

[Server(s) infrastructure 14](#_Toc376965634)

[Overview 14](#_Toc376965635)

[Server Hardware Requirements 14](#_Toc376965636)

[Server Software Requirements 14](#_Toc376965637)

[Data collection and storage, privacy rules 15](#_Toc376965638)

[Medical data 15](#_Toc376965639)

[Private data 15](#_Toc376965640)

[Public data 16](#_Toc376965641)

[Data storage/hosting scenarios 16](#_Toc376965642)

[Data exchange 17](#_Toc376965643)

[Data encryption, security and privacy 17](#_Toc376965644)

[Data model 17](#_Toc376965645)

[Development technologies 17](#_Toc376965646)

[HomePad 17](#_Toc376965647)

[ManagementPortal 18](#_Toc376965648)

[FriendsAndFamily Portal 18](#_Toc376965649)

# Preface

This document describes the requirements towards hardware platforms, communication protocols, and database of E Care@Home project (further eCH) with overall functional description. It also briefly describes security and privacy issues as long as it justifies a chosen platform. More extensive description of security and privacy requirements are covered in the separate deliverables D1.4a– “Security and privacy, patients’ rights” and D1.4b – ““Data storage, collection and access standards”.

According to the project application the objective of this deliverable is to identify the requirements which are not directly related to the functionality as such, but are used to provide the base for reliable, scalable and secure handling of the data flow within the solution.

 The deliverable document contains 4 main sections:

1. Solution architecture section and related Appendix 1 of this document, describing the overall solution scheme and requirements towards main solution products and hardware
2. Server infrastructure – server hardware and software requirements
3. Data collection, storage and security rules describing data and database related requirements. The database description and diagram are located in the separate document within this deliverable.

# Disclaimer on assumptions and limitations

The document contains system architecture description, applicable to be deployed in project partners’ countries – Netherlands, Norway and UK. As have been mentioned in the deliverable 1.4, even there are EEA standards and regulations adopted by all three countries, and Europe wide, there may be additional country specific rules and interpretations, as well as professional standards required to be followed in order to deploy the system not specifically described in this deliverable or deliverable 1.4.

In the document the additional functionality or requirements which are not mandatory to implement and follow are described in order to have a guidance for further implementation and commercialization of the developed products. These additional requirements are not essential however for realization of the use case scenarios mentioned in the project application, as well are not formal deliverables. Such requirements are marked as a requirements for version 2.0 (v2.0).

It also worth to note that during the pilot testing additional requirements towards architecture may arise, especially in terms of integrating with other systems or devices.

# Solution architecture

Solution architecture scheme is shown in APPENDIX 1.

The solution consists of the following integrated software components:

* Central Management portal
* HomePad
* Friends & Family Portal (Informal Care Portal)
* Smartphone portal (v2)

# Solution components requirements

## System deployment scenarios

There are following basic deployment scenarios, which affect system architecture:

1. "Full scale solution deployment" - for follow up of health and wellness condition by a care house, home user, nurses and other medical personnel on the go, members of home user's family and friends

2. Care house only deployment scenario - when users stay and receive care in medical institutions

3. Independent home users with or without connecting friends and family for following up

For the pilot test in the project Full scale deployment scenario will be used with the following assumptions/limitations:

* Emphasis on self-care, a home user will play the central role while role of clinicians will be limited to participation on video conferences (more) and reacting on alarms (less)
* Home visits by clinicians will not be a part of the pilot, as it also rarely happened before introduction of the solution

The communication flow diagram of various scenarios is show in the Appendix 2 of this document. The types of users and corresponding products with brief description are listed in the following table:

|  |  |  |
| --- | --- | --- |
| **Product** | **Main users** | **Notes** |
| HomePad | Senior citizens at home | Also relatives and other persons living with the main user can use the product |
| CMP | Care and health watch personnel, such as nurses or medical doctors (further - Staff Users) | It is also used for solution configuration by IT personnel and for managing the working schedules by administrative staff |
| FriendsAndFamily (Informal Care Portal) | Relatives and friends of HomePad users |  |
| Smartphone Portal (v2) | Senior citizens outside reach of HomePad, FriendsAndFamily Portal users on the go |  |

## HomePad

**Description**

 The users use HomePad for self registering its health condition and wellness performance. They also use HomePad for direct communication, such as video calling and messaging) with care personnel (staff users) and friends and family. Health readings can be registered manually by a home user or automatically collected from compatible health and wellness sensors. Home users get notified on alarming health conditions as well as alarms will be send to responsible care personnel (staff users).

It is assumed that HomePad users have little or no experience interacting with any kind of computers and software. It also assumed reduced visual and tactile abilities.

**Platform and technical framework**

As HomePad main platform tablet PC type of computers are used. It can be either Microsoft Windows 8 based devices or Android based devices. The requirements are listed below:

### HomePad General Hardware requirements:

**1.1**. **Display**:

**1.1.1.** 25.7 cm (10.1") 1280 x 800 pixels diagonal WXGA

**1.1.2.** Ultra- Wide-viewing angle (178 deg)

**1.1.3.** Capacitive multi-touch

**1.1.4.** Corning Gorilla Glass 2

**1.1.5.** ‘All black’ / dark grey design

**1.1.6.** Anti-smudge coating

**1.2.** **Dimensions** approx. 177 x 260 x 9.2 mm

**1.3.** **Weight** approx. 650g

**1.4.** **Construction**

**1.4.1.** Robust Aluminium body (black preferred)

**1.4.2.** 1m drop test (could be achieved with added cover/bumper)

**1.5.** **Processor**: 1.5GHz Quad core

**1.6.** **Storage** 16Mb

**1.7.** **Ram**: 2GB

**1.8.** **Graphics:** multimedia capable (Open GL over 500Mhz)

**1.9.** **Webcams**:

**1.9.1.** Front: 2MP

**1.9.2.** Rear: 5MP

**1.10. Audio**

**1.10.1.** SRS built in stereo

**1.10.2.** Headset port

**1.10.3.** Integrated microphone – ideally dual array (noise cancelling + beam forming)

**1.10.4.** Highest audio level possible within form factor

**1.11.** **Wireless**:

TCP/IP connection, WiFi b/g/n or better required, 3G optional, Bluetooth 2.0 (min), Bluetooth 4.0 recommended. WiFi is used as primary connection mean, 3G can be utilized as a backup way of communication. Virtual Private Network (VPN) is recommended for secure communications if the device is connected to public use network (Internet).

**1.11.1. WIFI** 802.11/b/g/n

**1.11.2.** Bluetooth 4.0 / inc low energy

**1.12.** **Battery**: 8hrs min /12hrs ideal (look at heavy duty cost options)

**1.13.** **Ports/controls**

**1.13.1.** Usb charging (will be connected via to ‘drop in contacts’ in jacket via cable loom )

**1.13.2.** Power key (will only be used for resets)

**1.13.3.** Good quality Microphone – able to support telephony

**1.13.4.** Headset port

### HomePad general software requirements

**2.1.** Android 4.2 or better or Windows 8 Pro

**2.2.** Google Chrome browser 30.0.1599 or better with full screen and kiosk mode enabled by default (Windows) or Chrome M31 Beta or higher release level, with custom HW access and boot script (Android)

**2.3.** Mic drivers able to support IP telephony (including Bluetooth headsets)

**2.4.** Drivers needed to play multimedia content

**2.4.1.** Flash (Windows only)

**2.4.2.** E-book formats – epub (v2)

**2.4.4.** All common Video formats (v2)

**2.5.** On board security/virus protection / comms encryption (v2)

**3. Charging jacket and dock (v2)**

**3.1.** Custom assembly (To be designed by Alloy Ltd).

**3.2.** Provides mounting for ‘drop in’ charging cradle style contacts

**3.3.** Covers a short cable loom from USB to cradle style contacts

**3.4.** Covers the screen

**3.5.** Improves grip and drop performance

**3.6.** Provides clear accurate ‘drop on’ location of tablet onto dock.

### HomePad software integration requirements

**4.1. General UX presentation** The UX is written as a web app in HTML5/CSS/Javascript. The code is optimized for the browsers based on Blink (ex WebKit) engine and should be fully supported by Google Chrome browser, Chromium browser both on Android 4.2 and Windows 8 Pro.

**4.1.1. Full ‘kiosk mode’ from boot - t**he device must present the HTML5 based UX full screen at all times, with no address bar or ‘browser’ scrolling bars. This functionality should be accessible from Chrome M31 (Android)/ 30.0.1599 (Windows 8) or better.

**4.1.2. Chrome or Chromium based ‘full HTML 5 functionality’ controlled by software.**

**4.1.2.1.** Browser based secure video calling (including Audio only)

**4.1.2.2.** Instant messaging

**4.1.2.3.** Alerts/reminders

**4.1.2.4.** Automatic synchronisation with customer databases

**4.1.2.5.** Smart caching to optimise UX speed (eliminate perceived latency)

**4.1.2.6.** Smart integration with graphics and capacitive touch detection

**4.1.3. No ‘access permission’ screens/pop ups** All the necessary HW functions must be accessible directly from the UX code without any security access permissions pop ups at any time, including ‘first boot’. Typical examples include Camera and Microphone.

**4.1.4. Touch performance**

**4.1.4.1.** Scrolling The UX/graphics integration strategy must ensure that UX scrolling has an ‘‘instantaneous, smooth glide feel’ matched to code that is native on the device

**4.1.4.2.** Touch reaction capacitive sensitivity & integration must be set very high to ensure instant, reliable touch detection for older users with dry skin conditions/poor circulation which can reduce conductivity in the finger.

**4.1.5. Screen rotation disable** The UX will only be viewable in landscape mode with the cameras at the top. Accelerometer based screen rotations need to be disabled.

**4.1.6. Custom Keypad Presentation (Qwerty and Numeric) (v2)** The integration solution must allow for an external keypad to be specified later. Initially this will be a standard design, but this will eventually be replaced by a custom design.

**4.2. Main HW modes (v2)** The integration solution shall provide the interface necessary for Hardware access from the web app using JavaScript plug-in calls to relevant native code (Java or C++). Wherever possible this should be done using existing open source code bases such as PhoneGap.

**4.2.1. User perceived ‘ON’**

**4.2.1.1.** **In Use**

**4.2.1.1.1.** Screen brightness set at user preferred level (via ‘settings)

**4.2.1.1.2.** Activated by user touch

**4.2.1.2.** **Rest**

**4.2.1.2.1.** Charging If no touch events or alerts for *T* minutes Screen brightness automatically drops to lower brightness level = (default value *X(charging)*  – user control via ‘settings’)

**4.2.1.2.2.** Battery only when rest mode detected and charging = none then brightness dims to value Y = % of default value X (rest charging)

**4.2.2. User perceived ‘OFF’**

**4.2.2.1.** **Endurance Mode (battery)**

**4.2.2.1.1.** Triggered automatically when battery level is below value Z (to be set as a default in WT)

**4.2.2.1.2.** Screen is off/black, wifi off, but wakes up periodically (exact period tba) to send a distress alert

**4.2.2.1.3.** Endurance mode to last as long as available HW config allow (target 2/3 days)

**4.2.2.2.** **Endurance Mode (charging)**

**4.2.2.2.1.** When charging current is detected but battery level is still below the level needed to escape Endurand, mode, behave as per Endurance mode but display a ‘charging’ icon alone in the middle of the black screen.

**4.2.2.3.** **Full Hardware Off.**

**4.2.2.3.1.** Automatic when HW drops below minimum level

**4.2.2.3.2.** Must allow ‘on’ when charging current detected

**4.3. Key HW transitions**

**4.3.1.1.** **Wake Up from any ‘OFF’ mode**

**4.3.1.1.1.** Triggered by detection of charging current

**4.3.1.1.2.** Triggered by power key press

**4.3.1.1.3.** Automatically boots directly into UX

**4.3.1.2.** **Amber level Low power detection**

**4.3.1.2.1.** Power level *X* that triggers alerts in the UX

**4.3.1.2.2.** Other possible HW changes to be considered if necessary

**4.3.1.3.** **Red level Low power detection**

4.3.1.3.1. Power level *X* that triggers transition into ‘endurance’ modes

**4.3.1.4.** **Hardware reset**

**4.3.1.4.1.** Triggered by the power key (in the event of frozen screen)

**4.3.1.4.2.** Transition to Full HW Off on first push

**4.3.1.4.3.** Transition back to ‘On’ reboot on second push

**4.4. Software Access to HW control capability and status information (v2)**

**4.4.1. WIFI**

**4.4.1.1.** Access to radio signal level to display in UX ( yes/no acceptable)

**4.4.1.2.** Agreed protocol to trigger ‘loss of signal’ alerts via UX

**4.4.1.3**. (this includes ability to send a remote ‘no signal’ alert)

**4.4.1.4.** UX access to library of available local WIFI connections

**4.4.1.5.** Access to WIFI registration via UX

**4.4.1.6.** Register to multiple WIFI ID’s and store passwords

**4.4.1.7.** Remember multiple WIFI ID + passwords ‘pre-sets’

**4.4.1.8.** Group presets into a ‘home roaming’ set

**4.4.1.9.** Automatically connect to strongest WIFI ‘pre-set’ in the roaming set (or do whatever is necessary to build 100% secure coverage via repeaters and shift seamlessly from one to the other).

**4.4.2. Bluetooth**

**4.4.2.1.** UX control of ‘discoverable’ status

**4.4.2.2.** UX control over ‘connected device’ list

**4.4.2.3.** control & display of Bluetooth device status

**4.4.2.4.** UX control of multiple device connections

**4.4.2.5.** Support multiple ‘ready live’ connections that connect automatically as soon as ‘remote device on’ is detected.

**4.4.3. Battery level access**

**4.4.3.1.** Custom UX Display of battery level

**4.4.3.2.** UX to detect low power warning thresholds and send alerts:

**4.4.3.3.** UX to send ‘amber’ alert when level falls below X%

**4.4.3.4.** UX to send ‘red’ alerts in endurance mode - when level falls below Y%

**4.4.4. Charging current detection**

**4.4.4.1.** Trigger ‘charging’ indications in ‘on’ and ‘endurance’ modes

**4.4.4.2.** Allow remote detection of charging status via other portals

**4.4.5. Screen brightness**

**4.4.5.1.** Allow custom User control in home pad UX

**4.4.5.2.** Allow level changes associated with HW mode: Rest/Endurance etc..

**4.4.6. Speaker**

**4.4.6.1.** UX screen control of Volume level

**4.4.6.2.** Incremental levels and Mute control

**4.4.6.3.** UX display of level

**4.4.6.4.** HW keys to be disabled

**4.4.7. Microphone**

**4.4.7.1.** UX mute control

**4.4.8. Cameras**

**4.4.8.1.** UX – front or rear ‘live’ toggle

**4.4.8.2.** For each camera

4.4.8.2.1. UX - 1 touch ‘on off’ control

4.4.8.2.2. UX status indication

4.4.8.2.3. UX mini ‘feedback’ display of ‘live’ camera

4.4.8.2.4. UX ‘‘shutter’ button to capture stills

4.4.8.2.5. UX ‘FILM’ button (and red light) to capture video out of calls

**4.4.9. System sounds**

**4.4.9.1.** Default Library: (final list to be agreed) (no user options)

**4.4.9.1.1.** Precise ‘button click’

**4.4.9.1.2.** Subtle ‘Qwerty’ click

**4.4.9.1.3.** Woosh for ‘arrow’ transitions

**4.4.9.1.4.** Test Reminder

**4.4.9.1.5.** Diary reminder

**4.4.9.1.6.** Amber alert

**4.4.9.1.7.** Red alert

**4.4.9.1.8.** Incoming message to home page

**4.4.9.1.9.** Incoming video call

**4.4.9.1.10.** Positive ‘target reached’

**4.4.9.1.11.** Task done

**4.4.9.1.12.** Task aborted ahead of completion

**4.4.9.2.** UX to offer user control over ‘on/off’ and 2/3 levels

**4.4.10. Accelerometer**

**4.4.10.1.** To detect and send alert if a serious impact is detected

**4.4.11. Remote control capability**

**4.4.11.1.** Users in remote location, given permission, need to access a ‘remote view’ of the Homepad UX via the friends and family or ‘Care management’ portals

**4.4.11.2.** Remote control of settings

**4.4.11.3.** Remote access to WIFI

**4.4.11.4.** Managing content

**4.4.12. Security status and control**

**4.4.12.1.** Device unique identification code (e.g. MAC address) to be available to UX

**4.4.12.2.** HW access status to be accessible via UX

**4.4.12.3.** Password entry to be accessible via UX

**4.4.12.4.** Facial recognition sw accessible via UX

**4.4.13. Android app access**

**4.4.13.1.** Access to the full android Play library via an ‘android ‘cut through’ popup window’ to be defined in the UX.

**4.4.13.2.** Access to a ‘downloaded android app’ field in UX

**4.4.13.3.** Android apps to run full screen with ‘back button’ to appear overlaid

**4.4.14. Std Chrome browser access**

**4.4.14.1.** Access to a std chrome browser running directly in Android to be provided via a ‘cut through’ popup window to be defined in UX.

**4.4.14.2.** Standard browser config is to have all downloads / cookies etc.. disabled

**4.4.14.3.** Default homepage set to google Chrome.

### Health and wellness sensors

Types: heart rate monitor, blood pressure monitor, weights, ...

Standards and certifications: IEEE 11073, Continua certification recommended.

 Network communication: Blootooth 2.0 or better (4.0 recommended) (pairable with relevant operating system), WiFi b/g/n or better.

## Central Management Portal (further - CMP)

**Description**

 CMP is used by Staff Users for the following purposes: to configure basic settings of the solution (manage users, services and tests to be performed, form templates, etc.), monitor health condition of Service Users and react on alarming conditions, to communicate with Service users via messaging or video calling, to perform pre- assessments of Service Users and to create care plans with service scheduling.

 At is assumed that Staff Users have minimal experience working with computers and software for those required to monitor Service users, and more advanced PC-literacy for system administrators or service schedulers.

**Platform and technical framework**

As CMP main platform desktop computers are used. CMP is a web application and accessed using a web browser. The requirements are listed below:

### Central Management Portal Hardware minimal requirements

* 1. **Display:**

**1.1.1.** 55.9 cm (22’’) 1920x1080 pixels diagonal Full HD recommended

**1.2. Processor:** 1.5GHz double core

**1.3. Free storage:** 1 GB

**1.4.** **RAM:** 4GB or more

**1.5.** **Graphics:** multimedia capable (OpenGL over 500 Mhz)

**1.6.** **Webcams:**

 **1.6.1.** Front: 2MP

**1.7.** **Audio:**

 **1.7.1.** Headset port, Headphones

 **1.7.2.** Microphone

**1.8.** Network:

 1.8.1. Ethernet port, TCP/IP connection 100 Mbps

### Central Management Portal Software minimal requirements

**3.1. Operating system:** Microsoft Windows 7.0 or newer, Linux (Debian/Fedora/Ubuntu/openSUSE) capable of running Chrome 31

**3.2. Browser:** Google Chrome 31 or Chromium 31

## Friends and Family portal and Informal Care portal (further - FFP)

The same technical requirements as for CMP apply to FFP.

FFP communicates normally over public use network (Internet), so users of HomePad has to give their consent to transmit sensitive data.

## Smartphone Portal (v2) (further - SP)

SP will display alerts directed to it, offer limited response options and basic messaging/comms.

SP is web based application for use with browsers supporting HTML5 standard. The same notes on the browser apply here, so initially use of Google Chrome will ensure that all functions are accessible. To simplify the use of the app, it is recommended to create a shortcut on phone desktops or to have it as a "home page".

### Smartphone Portal Hardware minimal requirements

* 1. **Display:**

**1.1.1.** 8.9 cm (3.5’’) 960x640 minimum, 1280x920 pixels recommended

**1.2. Processor:** 1.5GHz double core

**1.3.** **RAM:** 1GB or more

**1.4.** **Webcams:**

 **1.6.1.** Front: 2MP

**1.7.** **Audio:**

 **1.7.1.** Speaker

 **1.7.2.** Microphone

**1.8.** Network:

 1.8.1. 3G (HSPDA) or faster, Internet connection

### Smartphone Portal Software minimal requirements

**2.1. Operating System:** Android 4.1.2 of newer

**2.2. Browser:**  Google Chrome browser 31

# Server(s) infrastructure

## Overview

The overview of the solution components is shown in Appendix 1. Based on the number of end-users and the workload the requirements towards server hardware may vary. The requirements listed below are valid for the trial deployment. It is expected required that all required server software will be installed on a single physical server. Also as an option existing hardware infrastructure in pilot test organization location will be audited, to check the compliance and possibility of installation of the solution components.

### Server Hardware Requirements

**1.1. Processor:** Intel based I7 2700 K (3.8 GHz) or equivalent

**1.2. Storage:** HDD 100GB free disk space, RAID 1

**1.3. RAM:** 16GB

**1.4. Network:** TCP/IP connection 100 Mbps

### Server Software Requirements

**2.1. Operating System:** Microsoft Windows Server 2008 R2 Standard edition or newer

**2.2.** **Web Server:** Internet Information Services 7.5 or newer

**2.3. Data Server**: Microsoft SQL server 2008 R2 Standard Edition. Enterprise edition to be considered in case of build-in data encryption requirement. Express Edition is a minimum requirement and can be considered to be used in pilot deployment.

# Data collection and storage, privacy rules

As data storage, several options can be used, depending on customer demands and country of installation, as it affects security requirements. These requirements are described in deliverable D1.4. – “Security and privacy, patients’ rights”, and “Data storage, collection and access standards”. In this document requirements with considerable impact on solution architecture are described below.

It is also important to distinguish between sensitive medical data, private data, and data for public use. Different types of data are explained and listed for each particular product, indicating by ‘x’ the product where this data is available.

## Medical data

Requirements toward handling medical data are strictest among data types used in the solution. The data of this type can be collected by different type of users or can be collected by third party medical devices (e.g. sensors). The rules which are applicable towards medical data are described in detail in the deliverable D1.4 . Medical data items used in the solution are listed in the table below:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Data** | **HP** | **CMP** | **FFP** | **NP** | **SP** | **Notes** |
| Assessment results |  | x |  |  |  |  |
| Care (Service plan) | x | x | x | x | X | Also includes information about scheduled visits of medical personnel in a calendar |
| Test (measurements) results | x | x | x | x |  |  |
| Wellness data | x |  | x |  |  |  |
| Alerts | x | x | x |  |  | Including settings for alarms |
| Care notes | x | x |  | x |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

## Private data

Private data is any non-medical data intended for access by a creator user or other users who has explicit permission to access such data. Such access can be granted also for certain groups of users.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Data** | **HP** | **CMP** | **FFP** | **NP** | **SP** | **Notes** |
| User demographics and contact details | x | x | x | X | X |  |
| Care (Service plan) | x | x | x | X | x | Also includes information about scheduled visits of medical personnel in a calendar |
| Messages | x | x | x |  |  |  |
| Video calls | x | x | x | X |  |  |
| Photos | x |  |  |  |  |  |
| Notes to self | x |  |  |  |  |  |
| News set-up | x |  |  |  |  |  |
| Third-party services | x |  |  |  |  |  |
| Test measurements (configured tests to measure) | x | x | x |  | x |  |
|  |  |  |  |  |  |  |

It should be noted, that although in practice medical nature data can be collected or exchanged using functionality normally used to create a private data, - for example sending a short message with test measurements, or making a video call between a service user and staff user, discussing alerting medical conditions. Such data doesn’t however fall upon rules of handling medical data and users should be notified about it.

## Public data

Public data is a data which is normally available for broad public without explicit permission by a creator of the data.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Data** | **HP** | **CMP** | **FFP** | **NP** | **SP** | **Notes** |
| News contents | x | x |  |  |  |  |
| Health care guidance | x | X |  |  |  | Non user specific |
| Test descriptions | x | x | x |  |  | Non user specific |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

With user consent, any data, including medical data, can be made public (however normally anonymized), for example for gathering statistics on different treatment approaches, or for commercial purposes.

## Data storage/hosting scenarios

Depending on deployment requirements as well as country of deployment several data storage and hosting options are available. Choosing hosting strategy normally requires to take into account the following points:

1. End-users residence country. In some countries it may be required to physically locate all servers of the solution within the country of deployment or at least within EEA.
2. Use of commercial cloud-based servers. Normally it is not recommended to use commercial cloud servers for storing medical data, as an access to the data can be gained by non-authorized users and it is beyond the control of the parties responsible for the deployment. Use of cloud based servers however can be allowed for storing private data (such as photos or messages)
3. Requirements towards encryption and data transfer links. This point requires answering the question is it enough to have the secure connection encrypting all data between client and server (VPN), or is it also required to authenticate any request to services handling medical data in addition.
4. Size of end user base (number of end users)

It should be possible to physically store the data in different locations based on data type, for example to store certain personal data, such as pictures in the cloud servers and medical data on highly secure server of medical or care institution. The objective of such storage model is to decrease deployment and maintenance costs, while still maintaining required level of security.

## Data exchange

Software which is developed within eCH project will use proprietary standard for the data exchange between solution components, in order to utilize existing developments of the partners involved.

For medical data exchange with third party systems, it has been accepted that Web Services according to HL7 ver.3 should be developed. It has been discovered however, that due to organizational issues it will be not possible to integrate the solution products with third-party services at the pilot site prepared by the partners – VUA University of Amsterdam and InGeest.

## Data encryption, security and privacy

*Requirements are described in detail in deliverable D1.4 "Security, privacy and vulnerability risks"*

Before the pilot deployment existing it will be analyzed possibility to re-use existing security methods (e.g. use of single domain log-on, existing VPN and secure zone etc.)

## Data model

Data model is described in detail in the separate document, part of the deliverable D1.3 “Data model”.

# Development technologies

Several considerations have been taken into account for choosing development technologies, such as

* Existing developments – to reuse proven methods of development portable applications
* Sharing of similar functionality and GUI from one product to another, such as calendar and video calls are used in Management Portal, HomePad and FamilyPortal
* Strict requirements on GUI for HomePad and control of the native functionality of HomePad device (battery, connection, disk space etc.)
* Localization – in order to ensure that the solution can be adapted to any language market

## HomePad

UX of HomePad should be developed to comply with HTML5 standard which will ensure portability of the product. At the same time it should be ensured that the requirements mentioned in “HomePad software integration requirements” section will be met, in order to achieve decent user experience level. As it has been mentioned in that section as a web application, it will still provide “native” application experience and the web browser controls will be hidden.

Use of AngularJS is considered to make a clear split between the development of UI, business and data layers. This will simplify the cooperation between the partners (HOAS and Alloy) during the implementation of WP2.

Some of HomePad developments, such as calendar, video calling functionality, charts [including LifeChart] will be re-used in other products within the solution.

For certain use cases to ensure additional security use of VPN connection should be considered.

## ManagementPortal

To utilize the previous developments, Management Portal will be developed using ASP.NET and C#. The application will be completely web based, no any third-party plug-ins will be required.

For use outside health care organization network use of VPN should be considered.

## FriendsAndFamily Portal

The same approach as for HomePad will be used for the development of FriendsAndFamily portal, except that it is not required to have “native” application experience and it can be run from the browser. At the moment of submitting of this document it is required to have Google Chrome v31 or Chromium open source browser v31 or later. It is expected that more browsers will be supported due to increase of HTML5 support.

For certain use cases to ensure additional security use of VPN connection should be considered.