Project # 643735
www.do-change.eu

Overall Do CHANGE Ecosystem Infrastructure Architecture

[Deliverable 4.9 (D60), Revision 1.0]

Key Information from the DoA	
Due Date	30-Nov-2016
Type	Report
Security	Public

Description:

This document presents the overall architecture of the Do CHANGE ecosystem. It identifies the main use cases supported, the ecosystem's division into services, the high-level interfaces between these services and the overall approach to coordinating the identity and privacy preferences of end users associated with the services utilised within the ecosystem.

Lead Editor: Robert Smith (DOC) **Internal Reviewer:** Zhong-Wei Liao (ITRI)

Versioning and contribution history

Version	Date	Author	Partner	Description
0.1	07-Nov 2016	RS	DOC	Initial draft for review by project partners.
0.2	22-Nov 2016	RS	DOC	Corrected typos and other errors identified during initial review.
0.3	23-Nov 2016	MW	TU/e	Reviewer’s updates.
0.4	24-Nov 2016	RS	DOC	Final correction of minor types and formatting issues and added missing details to the “Deliverable context” table. Clarified the different between the Lifestyle and Behavioural data categories in Section 4.5.2.
1.0	25-Nov 2016	AB	SmH	Official release

Statement of originality:

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Executive Summary

This document serves two purposes. Firstly, it presents the use cases that Do CHANGE intendeds to meet. Secondly, it presents the top-level architecture that is intended to meet the functional requirements of the use cases identified. The architecture presented is a collection of services and supporting functions, which operate together to facilitate the delivery of care to a patient, with this involving the encouragement of behavioural change. The detailed design of the services is not covered here since it is addressed in other related documents. However, details are relevant to coordinated operation of the services, that is the assumed organisational / structural model, the form of identifiers used and a common model for trust and permission management are detailed in this document.

The aim in generating this document has been to specify the architecture that will be implemented for use in the 2nd phase of Do CHANGE field trials, along with the use cases that will be used to verify its functionality ahead of those clinical field trials.

Table of Contents

References 5

1. About This Document 6

1.1. Deliverable context 6

2. Use Cases Supported 7

2.1. The Collection of Clinical Data from Community Based Patients 7

2.2. The Collection of Food Related Sensor Data 7

2.3. The Collection of Personality and Lifestyle Data 7

2.4. The Collection of Activity Data 7

2.5. The Collection of Sleep Data 7

2.6. The Delivery of Core DOs 7

2.7. The Delivery of Responsive DOs 8

2.8. Access by Care Providers to Data from Different Sources in One Place 8

2.9. Control of Access to a Patient's Data in Accordance with their Wishes 8

2.10. Making Pseudonymised Version of All Relevant Data Available for Analysis and Research 8

3. Overview 9

4. Concepts and Models 11

4.1. Introduction 11

4.2. Data Controller 11

4.3. Organisational Structural Model 11

4.4. Identifiers 12

4.4.1. Introduction 12

4.4.2. Plain Text Identifiers 12

4.4.3. Pseudonymised Identifiers 13

4.4.4. Preserving Anonymity 13

4.5. Trust and Permissions Model 14

4.5.1. Roles 14

4.5.2. Data Categories and Attributes 14

4.5.3. Data Access Types 14

5. Do CHANGE Phase 2 Architecture Details 15

6. Conclusion / Future Work 17

References

[A]	Key definitions of the Data Protection Act - https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/
[B]	Do CHANGE Data Dictionaries and Third Party Interfaces Design
[C]	The Identity and Permissions Management Framework Design
[D]	Do CHANGE Application Programming Interfaces Design

1. About This Document

Do CHANGE aims to develop and provide a health infrastructure for integrated disease management of citizens with high blood pressure and patients with ischemic heart disease or heart failure. In this context, it aims to give them access to a range of personalized health services intended to encourage behaviour change and to allow their behaviour and clinical parameters to be monitored, with the information collected being shared amongst the health services in a manner that reflects the citizens wishes and aims to optimise their health and well-being. This documents presents the architecture of the Do CHANGE health infrastructure, which facilitates the coordinated operation of the health services in accordance with the aims of the Do CHANGE project.

1.1. Deliverable context

Project item	**Relationship**
Objectives	This document is linked to the following WP4 objectives: To Specify and develop the overall Do CHANGE Ecosystem Architecture, both the services & component infrastructure, the data infostructure and its semantics. • The Data collection, storage, management and communication will take place in a secure patient controlled environment and feedback on transactions will be fed back to the individual. • All incoming data will be semantically tagged such that background knowledge, context and precise meaning are stored with the data and will inform any use of the data and its analytics.
Exploitable results	This part of the project is service design. It is anticipated that the services developed from this design would be further developed to commercially exploitable systems.
Work plan	This deliverable is associated with Task 4.1 in Work Package 4.
Milestones	This deliverable is not linked to an overall project milestone but does mark the submission of D4.9 (D60).
Deliverables	This document presents the overall architecture of the Do CHANGE ecosystem. It is linked with related deliverables that specify the design of subsystems defined this this document.
Risks	By having this document available, the risk of failure of the technology supporting the Do CHANGE phase 2 trails due to incompatibility of its components, or it not meeting end user needs, should be reduced.

2. Use Cases Supported

The architecture presented in this document is intended to support the use cases specified in Section 2, which have been identified by the Do CHANGE consortium.

2.1. The Collection of Clinical Data from Community Based Patients

This use case concerns the collection of both physiological measurements and symptomatic measures from patients that are based at home, where the patient is not supervised by a clinician whilst the data is being recorded. For the target conditions, key physiological measures include blood pressure and ECG.

2.2. The Collection of Food Related Sensor Data

This use case refers to the collection of data from sensors related to the food and fluids that the patients consume. Specifically, this concerns food composition measures derived from impedance sensors and photographs, as well as measurements made of the volume of fluid consumed by the patient.

2.3. The Collection of Personality and Lifestyle Data

This use case concerns the collection of a broad range of measures made once or periodically using "instruments" in the form of questionnaires. A specific example is the "Pre-DO" questionnaire employed to seed the algorithm for the delivery of "DOs" to patients, which are messages that are intended to stimulate behaviour change.

2.4. The Collection of Activity Data

This use case concerns the collection of data related to the level of movement made by the patient during the hours that they are awake. In the context of Do CHANGE, it relates to movement sensors both from systems provided within the consortium and those by third parties.

2.5. The Collection of Sleep Data

This use case concerns the collection of data related to the quality of sleep that patients have. Like activity data, in the context of Do CHANGE, it relates to movement sensors both from systems provided within the consortium and those by third parties.

2.6. The Delivery of Core DOs

This use case concerns sending patients messages that are intended to stimulate behaviour change, where the content of these messages and their scheduling are determined from the patient's responses to a personality and lifestyle profiling "instrument" called the "Pre-DO".

2.7. The Delivery of Responsive DOs

Like the delivery of core DOs, this use case concerns sending patients messages that are intended to stimulate behaviour change. However, for this use case, the content of these messages and their scheduling are determined from the on-going data collected from the patient in a feedback loop, which aims to maximise the effectiveness of the DOs.

2.8. Access by Care Providers to Data from Different Sources in One Place

This use case concerns the ability of care providers to access in once place relevant data relating to a patient that is obtained from different sources and provided in accordance with the care provider's role and the wishes of the patient. A specific example is to combine activity data from third party systems and food sensor data with clinical data, allowing a clinician to make a comprehensive assessment of a patient, considering a wide range of factors that may impact their health state.

2.9. Control of Access to a Patient's Data in Accordance with their Wishes

This use case concerns giving the patient control over access to data collected from them. It involved providing patients with mechanisms to control "who" can access (specified by organisation, role and possibly individuals) and what they can access (specified by information type / classification).

2.10. Making Pseudonymised Version of All Relevant Data Available for Analysis and Research

This use case concerns making data collected on patients from many diverse sources available in pseudonymised format, that is so that the data can be seen to all relate to an individual while maintaining the anonymity of that individual with respect to most those who have access to the information. Note that, where the patient has authorised access by organisations or persons, a mechanism should be available to allow them to identify the patient from their pseudonymization identifier so that appropriate interventions can be made is appropriate from the results of analysis or research.

3. Overview

An overview of the Do CHANGE system architecture is presented in Figure 1.

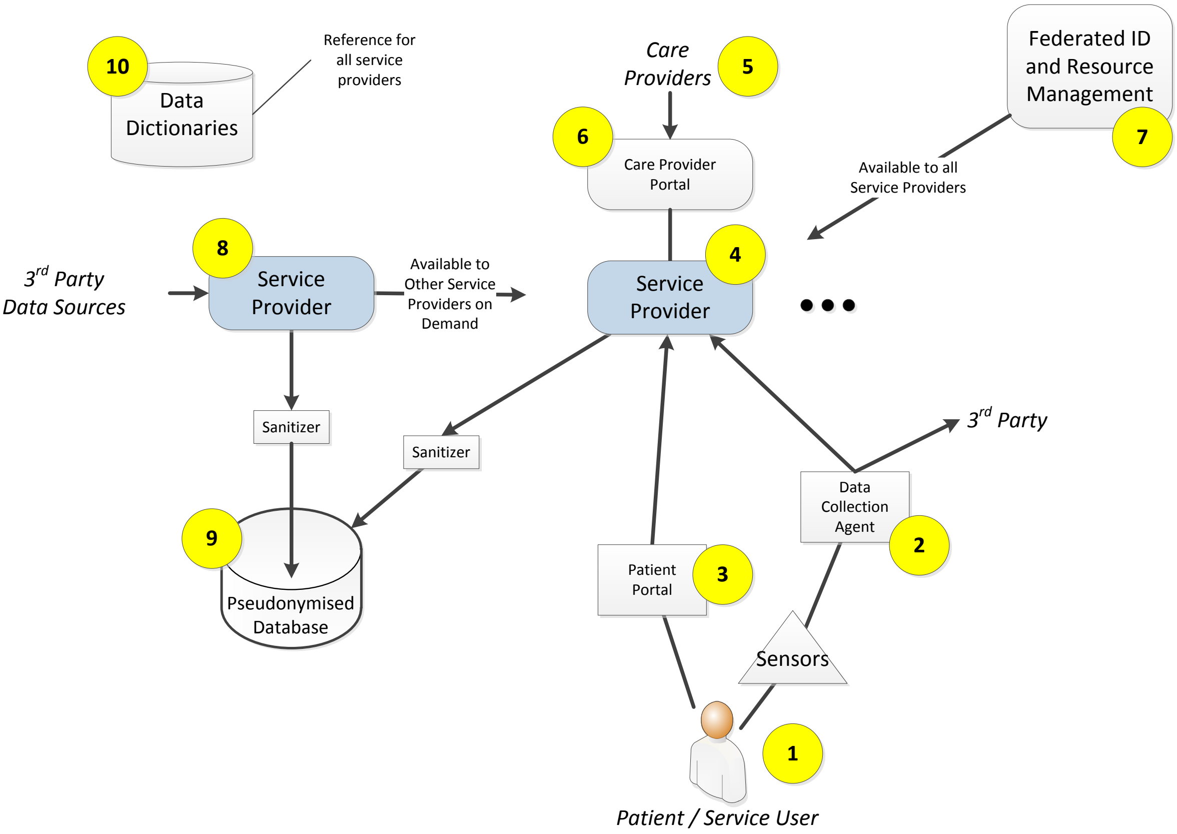

Figure 1 System Architecture Overview

The key elements are identified by highlighted numbers. These are as follows:

1. **Patient / Service User** is the subject of care provision. They have sensors that measure relevant environmental, physiological or activity parameters.

2. A **Data Collection Agent**, facilitates the collection of the data generated by the sensors and transfers this to a remote system, which may be a DoCHANGE Service Provider or a 3rd party system.

3. A **Patient Portal** allows interaction between the patient and a Service Provider. This may be used to allow non-sensor data to be collected such as symptomatic and well-being measures, to provide motivational messages to be presented to the Patient / Service Users and / or to allow the Patient Service User to control access to their information.

4. There are several DoCHANGE specific **Service Providers**, each providing specialised services such as clinical data collection, managing dedicated sensors and the generation of life style change motivational messages,

5. **Care Providers** supervise the care of Patients / Service Providers.

6. **Care Provider Portals** are the means by which Care Providers interact with the Service Providers and therefore the Patients / Service Users in their care.

7. A special **Federated ID and Resource Management** service allows the Service Providers to operate in a coordinated manner with respect to sharing information and resources relevant to the care of the Patients / Service Users. This works in unison with identity and resource management local to each service provider such that the preferences of the Patient / Service User in terms of information sharing are respected.

8. A special **Third Party Data Aggregator** Service Provider allows data from 3rd party systems to be made available to all relevant and authorised Service Providers in such a way that, it is linked to the Patient / Service Users they are currently dealing with and is in accordance with the Patient / Service Provider's wishes.

9. A **Pseudonymised Database** retains a sanitised version of all information collected and authorised by Patients / Service Users for anonymised use in research. Within this database, the information is only linked to the associated patient by a pseudonymised identifier, thereby maintaining the confidentiality of the Patient / Service Users. The information in this database can be subject to complex, 'big data' analysis techniques with the aim of identify patterns that can be used to enhance the care of individual Patients / Service Users or the whole population.

10. **Data Dictionaries** are maintained that relate to coding of the diverse information collected. These are based on relevant standards such as HL7 where available and relevant. Otherwise, new encodings are published. This facilitates tagging for wide scale understanding of the information when used for automated analysis.

4. Concepts and Models

4.1. Introduction

This section presents several concepts and models that are employed within the Do CHANGE architecture.

4.2. Data Controller

A Data Controller is defined as follows (Ref. [A]):

> "A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed."

In the context of the Do CHANGE architecture, the Data Controller corresponds to the organisation and / or specific persons within an organisation, who have control and/or responsibility for providing access to personal data. Hence, this could be a patient themselves (if they have full control over their data), and / or appropriate persons within the organisations providing IT services to them, or these organisations as a whole. Also, a given patient may have different types of information distributed between systems and services, so for that patient there may be several Data Controllers, each of a different type of data.

4.3. Organisational Structural Model

Within the scope of this document, a hierarchical structure of systems and organisations is assumed as indicated in Figure 2.

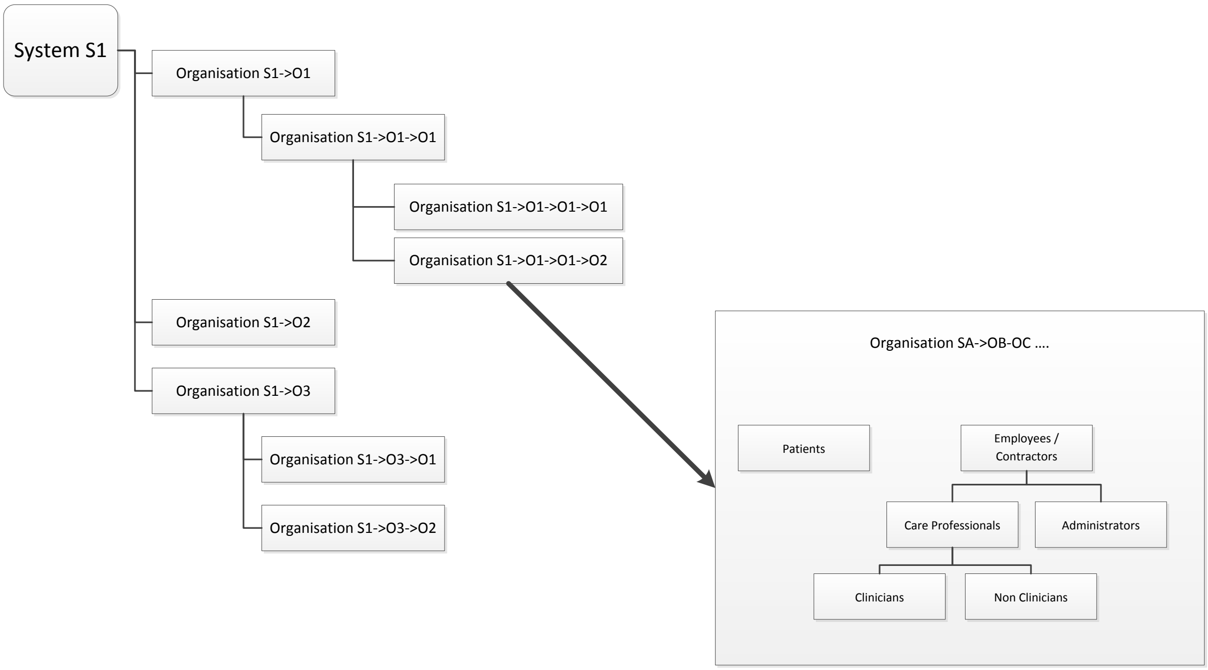

Figure 2 Organisational Hierarchy

In Figure 2 there is a system S1 at the top of the hierarchy. This is one of several systems providing health services, each of which could operate stand alone or in collaboration with other systems. Within the system there is a hierarchy or organisations, starting with in this case three top-level organisations S1->O1, S1->O2 and S1->O3. These top-level organisations may have sub-organisations, which in turn may have sub-organisations. For example, in an acute care context, the top-level organisations might be regional health care providers, their sub organisations hospitals and, the sub organisations of the hospitals clinics. In addition, each organisation will in general have several different categories of person associated with it, which in-turn can be viewed as being in a hierarchy. At the top-level, there are Patients and Employees / Contractors (the staff of the organisation). The later then divides into care professionals and administrators. Finally, the care providers divide into clinical staff and non-clinical staff.

4.4. Identifiers

4.4.1. Introduction

Within the Do CHANGE architecture, identifiers correlate to entities within the organisational structure model specified in Section 4.2. Hence, identifiers may correspond to entities which are and one of the following:

- a service, that is an IT element providing a date related service;
- a system, that is an IT element providing one or more services;
- an organisation, that is an organisation, which may exist within a hierarchy as outlined in Section 4.2;
- a person within an organisation.

4.4.2. Plain Text Identifiers

The Do CHGANGE architecture employs plan text identifiers, that is ones in which anonymity of persons is not guaranteed. These take the form of email address with the following structure:

<PersonID>-<OrgID>@<ServiceID>.<SystemID>.<DomainID>

Where:

PersonID is an optional element that identifies a person. It may contain any characters for a valid email except '–' and '@'. If this element is absent, then all persons within the scope determined by the other elements of the identifier are assumed to be covered by the identifier where appropriate.

OrgID is a mandatory element that identifies an end user organisation. It may contain any characters for a valid email except '–' and '@'. If required, the special value *everything* can be used to specify all organisations in the context of a system or service.

ServiceID is an optional element that identifies a service. It may contain any characters for a valid email except '.' and '@'.

SystemID is a mandatory element that identifies the IT system contextualising the identifier. It may contain any characters for a valid email except '.' and '@'.

DomainID is a mandatory element that identifies the own provider of the IT system. It may contain any characters for a valid email except '.' and '@'.

Some examples are:

jim.jones-DoCHANGE_ES_Hospital1@dochange.docobo.net – This specifies an individual, within the organisation DoCHANGE->ES->Hosiptal1, for the service Do CHANGE hosted by Docobo in the domain net

DoChange_ES_Hospital1@dochange.dsd.me – This specifies an the whole of the organisation DoCHANGE->ES->Hosiptal1, for the service Do CHANGE hosted by DSD in the domain me.

everything@dochange.tue.nl – This specifies an individual, the service Do CHANGE hosted by TU/e in the domain nl.

4.4.3. Pseudonymised Identifiers

The Do CHGANGE architecture employs plan text identifiers, that is ones in which anonymity of persons is guaranteed, such that only the Data Controller can identify the actual person associated with the pseudonymised identifier (where appropriate). These have form of an ASCII string. Some examples are as follows:

5804bc70f6c72a7451e0ce9e – a GUID / UUID;

EucMw9PGqGEMwuzKO3hO2LW1DPNtQFYn – a token (often used in http headers in various forms);

37306 96311 – a numeric identifier.

4.4.4. Preserving Anonymity

To preserve anonymity with a system that have sensitive information shared across different subsystems, as indicated in Figure 3, the best practice approach is that the Data Controller should provide each system with a different pseudonymised identifiers to each of its cooperating peer systems.

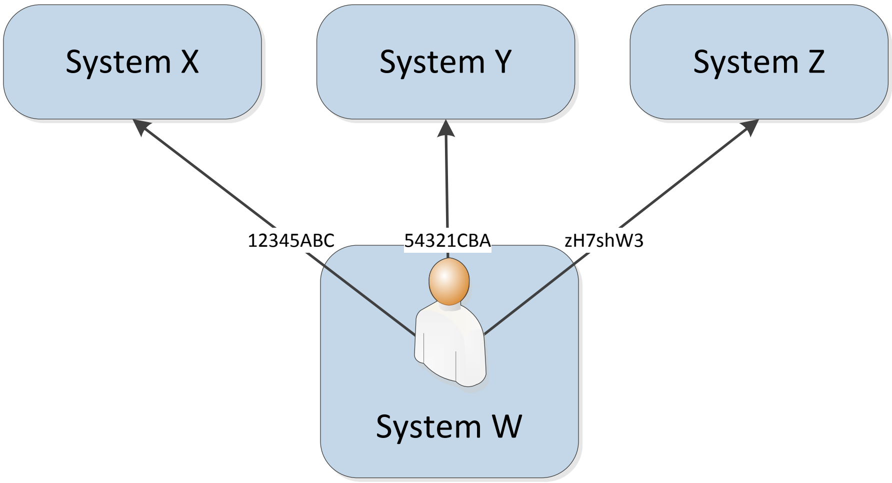

Figure 3 Using Different Pseudonymised Identifiers

4.5. Trust and Permissions Model

4.5.1. Roles

The following roles are used within the Do CHANGE architecture:

- **Patient** - a patient;
- **Care Provider (Clinical)** - a provider of clinical care;
- **Care Provider (Not Clinical)** - a provider of non-clinical care;
- **Researcher** - a researcher;
- **Administrative** – a person / organisation undertaking an administrative role.

In addition, a virtual role **ALL** is used, which incorporates all the above.

4.5.2. Data Categories and Attributes

The following data categories are used within the Do CHANGE architecture:

- **Demographics** - demographical data relating to individuals;
- **Clinical** - clinical data relating to individuals;
- **Lifestyle** - lifestyle data relating to individuals,
- **Behavioural** - behavioural data relating to individuals, that is, measurements derived from sensors that are not primarily intended for clinical use.
- **Social** – social data relating to individuals.

Furthermore, each category may be supplemented by the attribute *Sensitive*, indicating that the associated information is sensitive. The absence of this attribute implies that the data is sensitive.

In addition, a virtual category **ALL** is used, which incorporates all the above.

4.5.3. Data Access Types

The following data access types are used within the Do CHANGE architecture:

- **View** – viewing of the data is permitted;
- **Edit** – editing (modifying / updating) of the data is permitted;
- **Add** – the creation of new data is permitted;
- **Delete** – the deletion of existing data is permitted
- **Full** – there are no restrictions on access.

5. Do CHANGE Phase 2 Architecture Details

A specific configuration of the generalised architecture is presented in Figure 1 is to be utilised for the Do CHANGE phase 2 trials, this is presented in Figure 4. This is based on a set of Do CHANGE specific services, some of these (OMNI, DSD and doc@HOME) being specific to the patient-orientated services provided by the associated Do CHANGE partner, the others being associated with the federates / corporative operation of these services.

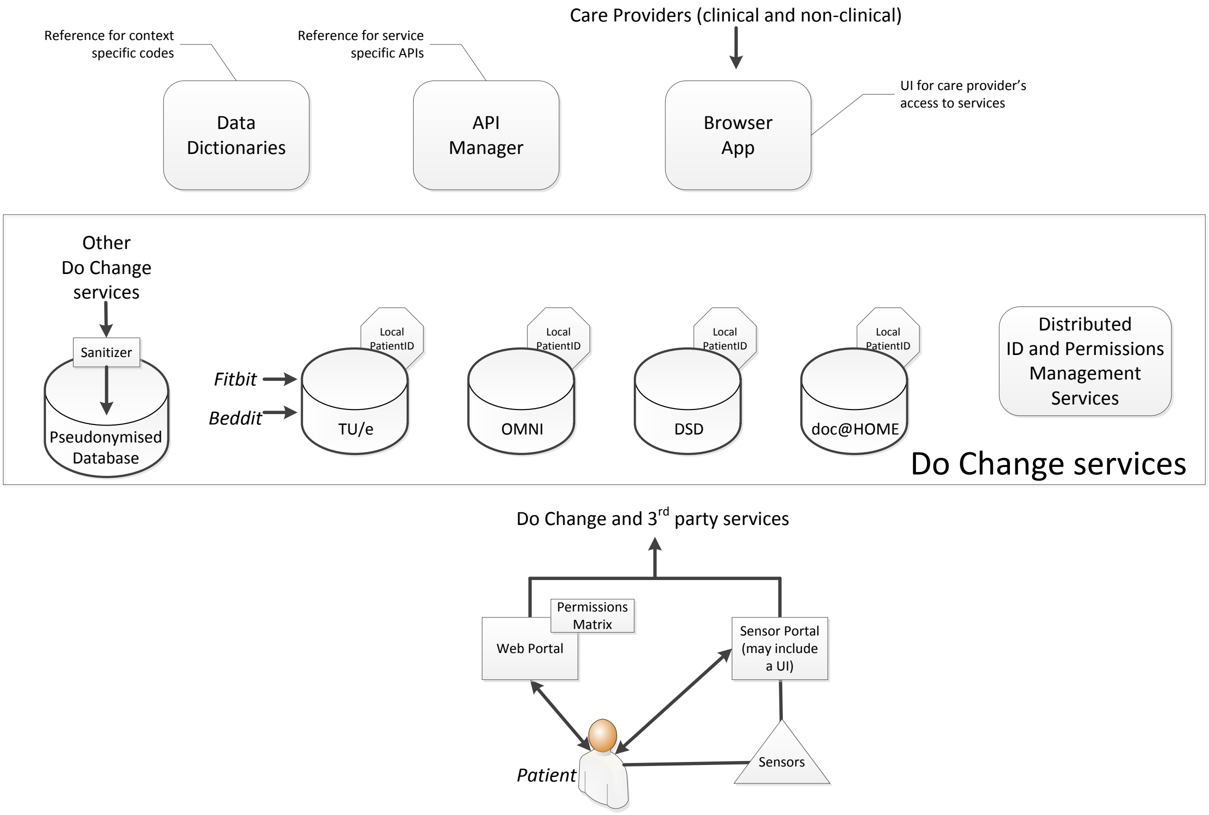
Care Providers (clinical and non-clinical)
Reference for context specific codes
Reference for service specific APIs
Data Dictionaries
API Manager
Browser App
UI for care provider's access to services
Other Do Change services
Sanitizer
Pseudonymised Database
Fitbit
Beddit
Local PatientID
TU/e
OMNI
DSD
doc@HOME
Distributed ID and Permissions Management Services
Do Change services
Do Change and 3rd party services
Permissions Matrix
Web Portal
Sensor Portal (may include a UI)
Sensors
Patient

Figure 4 Phase 2 Architecture

The federated services include the identities and permissions service, the functionality of which is distributed amongst the other services, with its function being to encode the patient's wishes with respect to access to their data and to ensure these are honoured and aims to control access The other federated service is the pseudonymised database. For patients that have consented to share their anonymised data for research purposes, this stores that data using a pseudonymised identifier, which allows data from difference sources to be identifies as being associated with the same patient and allows original Data Controllers to identify the actual patient associated with the data.

The Do CHANGE services shown in Figure 4 are provided to support a community based patient who, in general, may have sensors specific to their needs with a local portal routing sensor data to the associated service provider (which may be a 3rd party). The portal may or may not have a user interface. In addition, the patient has access to a web -interface through which they can control access to their information, based on the model presented in Section 4.5.

Care providers access the services via a web-interface. These may be providing clinical care or non-clinical care and have access to patient data in accordance with the patient's wishes. Depending upon the service and the patient, that access may be fully controlled via the patient's web interface from initiation of their use of the associated service. Alternatively, it may have been seeded based on a paper consent form they sign when first receiving the service, with the web interface giving them and / or their family/lay carer/ partner, the ability to update these initial settings.

The Data Dictionaries element indicated in Figure 4 is a shared reference for data encoding that is used when no appropriate existing encoding is available. This has interfaces to allow lookup and update of the reference. More details are provided in the separate document Do CHANGE Data Dictionaries and Third Party Interfaces Implementation Report.

The API Manager element indicated in Figure 4 is a reference for the APIs used by the different services. This has interfaces to allow lookup and update of the reference. More details are provided in the separate document Do CHANGE Data Dictionaries and Third Party Interfaces Design (Ref. [B]).

6. Conclusion / Future Work

The architecture presented in the later part of this document provides a basis for fulfilling the use cases present at the start of the document. When combined with the following, related documents:

- Do CHANGE Data Dictionaries and Third Party Interfaces Design (Ref. [B]);
- The Identity and Permissions Management Framework Design (Ref. [C]);
- Do CHANGE Application Programming Interfaces Design (Ref. [D]).

A design is specified that will allow the Do CHANGE partners to provide an implementation of the architecture suitable for validation in field trials. Hence, the next milestone to be reached is a to implement the services specified in the architecture and to verify that they cover the functional requirements of the use cases.