DiADeM Service Definition

1. Contents

2. Definitions

The definitions of abbreviations and terms used in this document are detailed below.

ITEM	DEFINITION
Access	Actions that may result in: (i) the data being viewed or changed; (ii) operational aspects of IT systems to changed; or (iii) security settings of IT systems to viewed or changed.
Agreement [1]	DiADeM Service Use Agreement: Main
Agreement [2]	IT Services Agreement
Agreement [3]	DiADeM Service Use Agreement: Apperta-User
Agreement [4]	Data Processing Agreement: Apperta-inidus
Agreement [5]	Data Processing Agreement: User- inidus
Apperta	The Apperta Foundation C.I.C., Company registered in England and Wales registration number: 09483987, Registered address: 10 Queen Street Place, London, EC4R 1BE
Apperta Data and Systems	(i) any DataDC for which Apperta is the Data Controller; and (ii) all Apperta IT Systems
Apperta IT Systems	All IT systems that Apperta controls to undertake Processing of DataDD where: (i) processing includes management of the data processing; (ii) the IT systems are under the control of Apperta; and (iii) IT Systems include DiADeM Web Service Tools.
Apperta Personnel	Those persons directly employed by Apperta; and subcontractors and agents working under Apperta's direct control
Assessor	This is a User role, where the User is registered to carrying out the DiADeM assessment on patients.
Breach of Personal Data	A breach of personal data means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.
CDR	Clinical Data Repository

CESG	Communications-Electronics Security Group. This is is now part of National Cyber Security Centre (https://www.ncsc.gov.uk/). The UK government's National Technical Authority for Information Assurance (CESG), advises organisations on how to protect their information and information systems against today's threats.
Data Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, as defined by Article 4 of the GDPR.
Data Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, as defined by Article 4 of the GDPR.
Data Protection Officer (DPO)	Information Governance Role, defined under Article 39 of the GDPR.
Data Subject	A natural person who is the owner of the Personal Data
DataDC	Data that is controlled by the Data Controller
DataDD	Any data that is stored on the DiADeM Service.
DiADeM	Diagnosing Advanced Dementia Mandate, a dementia diagnostic tool to support the diagnosis of people living with advanced dementia in care home settings. It is designed for use on people living with advanced dementia within a care home who do not have a formal diagnosis. In these cases a referral to memory services may not be feasible or desirable, and is likely to be distressing for the individual.
DiADeM app	The app that the Assessor downloads to their remote device which they use to undertake the DiADeM Assessment.
DiADeM Assessment	A tool that has been developed in 2015 by the Yorkshire & Humber Dementia and Older Peoples Mental Health Clinical Network (YH DOPMH CN) with input from a range of stakeholders including experts in the field of Dementia from across the health spectrum and in particular from Dr Graeme Finlayson and Dr Subha Thiyagesh who shared their existing protocols. The application has support from the Alzheimer’s Society and its use for diagnosing Dementia in the care home setting has been recommended by Professor Alistair Burns the National Clinical Director for Dementia and Older People’s Mental Health.
DiADeM Assessment Report	the report generated as an outcome of a completed DiADeM Assessment. This report is in a pdf format and the Assessor sends this to their selected

	Recipient.
DiADeM Authentication Service	The Authentication Service holds User information for the purposes of managing permitted access and sharing of information held by the Diadem Service.
DiADeM CDR Service	The CDR Service is used to hold patient data (includes sensitive data). It comprises the CDR server and demographics server.
DiADeM Service	The Diadem Service are the full suite of services through which the DiADeM is delivered to Users.
DiADeM web portal	The web portal through which Users gain access to the Diadem Service.
DiADeM Web Service Tools	The tools provided through which the User accesses the Diadem Service.
DPcdr	The Data Processor of the DiADeM CDR Service
DPIA	Data Protection Impact Assessment (refer to Article 35 of GDPR, and https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/)
ITServices	All IT services that inidus provides to support the DiADeM Service
ehrID	The unique internal identifier for a single patient, created by the DiADeM CDR Service
GDPR	General Data Protection Regulations (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1490179745294&from=en)
Information Commissioner's Office (ICO)	refer to https://ico.org.uk/
inidus	inidus Limited, Company registered in England and Wales registration number: 10733421, Registered address: The Oakley, Kidderminster Road, Droitwich, WR9 9AY
inidus Data and Systems	(i) any DataDC; and (ii) all inidus IT Systems
inidus IT Systems	All IT systems that inidus controls to undertake Data Processing of DataDD, including management of the data processing, where the systems are under the control of inidus
inidus Personnel	Those persons directly employed by inidus; and subcontractors and agents working under inidus' direct control
non-Clinical Auditor	This is a User role, where the User is able to obtain reports based on the full data held by the DiADeM Service. All reports are processed such that they contain NO patient Personal Data
Person identifiable Data (PID)	This is the same as Personal Data
Personal Data	Any data relating to an identified or identifiable natural person, as defined by Article 4 of the GDPR, that is stored on the inidus platform
PurposeDP	For inidus to discharge inidus’ obligations as Data Processor of the DiADeM

	CDR Server
Privacy Impact Assessment (PIA)	Privacy Impact Assessment. This is defined under the Data Protection Act (refer to https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf). Note that, under the GDPR, the PIA is replaced by the DPIA.
Recipient	This is a User role, where the User is a clinician responsible for the long term care of the patient, or works for a clinician who is responsible for the patient’s long term care. A Recipient is a person to whom an Assessor is able to send a DiADeM Assessment Report.
Retention Period	The time period that Personal Data is held by the DiADeM Service, after which point it being deleted.
Sensitive Data	Referred to as a special category of Personal Data within Article 9 of GDPR, and includes health data
Third Party	All persons or organisations who are not party to the agreement. Where one of the party is "inidus", then Third party excludes all inidus Personnel
User	The person who has registered on the DiADeM system to use the Diadem Service
User Role	The role that the User is registered on the Diadem Service. A User may register under one or more of the following roles types: (1) Assessor (2) Recipient (3) non-clinical Auditor
Working Hours	Working hours are defined as 9 a.m. to 5 p.m. on Monday to Friday, excluding bank holidays

3. Purpose of Document

The purpose of the document is to provide an overview of and introduction to the **DiADeM Service**. The intended audience are the **User**’s of the service, and NOT the patients who are to be assessed.

4. Introduction

4.1. Background

DiADeM (Diagnosing Advanced Dementia Mandate) is a dementia diagnostic tool to support the diagnosis of people living with advanced dementia in care home settings.

It is designed for use on people living with advanced dementia within a care home who do not have a formal diagnosis. In these cases a referral to memory services may not be feasible or desirable, and is likely to be distressing for the individual. Despite this, a formal diagnosis may still be beneficial to the patient, their families and carers - the **DiADeM** tool fills this purpose.

The tool was developed in 2015 by the Yorkshire & Humber Dementia and Older Peoples Mental Health Clinical Network (YH DOPMH CN) with input from a range of stakeholders including experts in the field of Dementia from across the health spectrum and in particular from Dr Graeme Finlayson and Dr Subha Thiyagesh who shared their existing protocols. The application has support from the Alzheimer's Society and its use for diagnosing Dementia in the care home setting has been recommended by Professor Alistair Burns the National Clinical Director for Dementia and Older People's Mental Health.

The YH DOPMH CN considered that an electronic version of the **DiADeM** tool would be useful, and they teamed up with Code4Health to develop an electronic version of the **DiADeM** tool - a **DiADeM app** - that can be used on a variety of handheld and portable devices. A small steering group which includes the YH DOPMH CN's GP Dementia Adviser, representatives from Code4Health, Application Insight (this is the app developer) and YH DOPMH CN staff, has been working towards getting a Public Beta version ready including testing prior to launching the App and making it available to all.

4.2. Who is intended to use the **DiADeM Service**?

(1) Clinical Assessment

The **DiADeM Service** is intended to be used by persons with suitable clinical training and qualification.

An **Assessor** undertakes a patient assessment, using the **DiADeM app** which is installed on their remote device (e.g. tablet). The **DiADeM app** prompts the **Assessor** in all aspects of the **DiADeM Assessment**, and the **Assessor** records all assessment results directly into the **DiADeM app**.

During the Assessment, the **Assessor** is require to interview an Informant and records responses on the **DiADeM app**. The Informant provides a corroborating view of the patient. The questions to the Informant are non-clinical in nature.

When the **DiADeM Assessment** is complete, the **Assessor** uses the **DiADeM app** to email the completed **DiADeM Assessment Report** to the **Recipient**. The **Recipient** (or the **Recipient**'s organisation) is responsible for the long term clinical care of the patient.

(2) Audit

The **DiADeM Service** allows a category of use "**non-clinical Auditor**" to register. This **User** is able to create usage reports for the **DiADeM Service**. Whilst the underlying tools can access the underlying **DiADeM** patient **Personal Data**, the **non-clinical Auditor** is not able to see any of the underlying data, and all information seen by the **non-clinical Auditor** is anonymised and contains no **Personal Data**.

4.3. Parties involved in the Delivery of **DiADeM**

Party	**Role**
Yorkshire & Humber Dementia and Older Peoples Mental Health Clinical Network (YH DOPMH CN)	**DiADeM** Sponsor; Subject Matter Experts in the dementia assessment
Code4Health	NHS Customer - commissioning development of **DiADeM** solution
Apperta Foundation CIC	Administrator of the **DiADeM Service**. **Data Controller** of **User Personal Data**
inidus	**Data Processor**
User	This is a **User** Role. There are presently three **User** roles - Accessor, **Recipient** and non-clinical Auditor. **Data Controller** of patient **Personal Data**.
Patient	The person undergoing the **DiADeM Assessment**
Informant	A person able to provide corroborating history of the patient. During the **DiADeM Assessment**, an "informant" is asked questions of non-clinical nature, about the patient.
Application Insight	The software developer of the **DiADeM appl**ication

5. Operation

5.1. Registration

The **DiADeM Service** is offered to **User**s via the **DiADeM Web Portal**. All **User**s are required to register prior to their first use of the **DiADeM Service.** The portal enables **Users** to register to use the **DiADeM Service** and to manage their registration if their personal details or roles change.

5.2. **Apperta**

Apperta is the administrator of the **DiADeM Service**. In this capacity, **Apperta** is in overall control of the **DiADeM Service** offered to **Users**.

5.3. **User** Role: **Assessor**

The **Assessor** is a **User Role**. The **Assessor** carries out the **DiADeM Assessment** of the patient in real time using the **DiADeM app** operating on their remote device. On completion of the **DiADeM Assessment**, the **Assessor** selects a **Recipient** on the **DiADeM app**, and emails the completed **DiADeM Assessment Report** to the **Recipient**.

5.4. **User** Role: **Recipient**

The **Recipient** is a **User Role**. The **Recipient** receives completed **DiADeM Assessment Report**s by email from the **Assessor.** The **Recipient** is required to be the clinician who is responsible for the long term care of the patient. The **Recipient** may also be an administrator working on behalf of the clinician responsible for the long term care of the patient and following agreed local protocols.

5.5. **User** Role: non-clinical Auditor

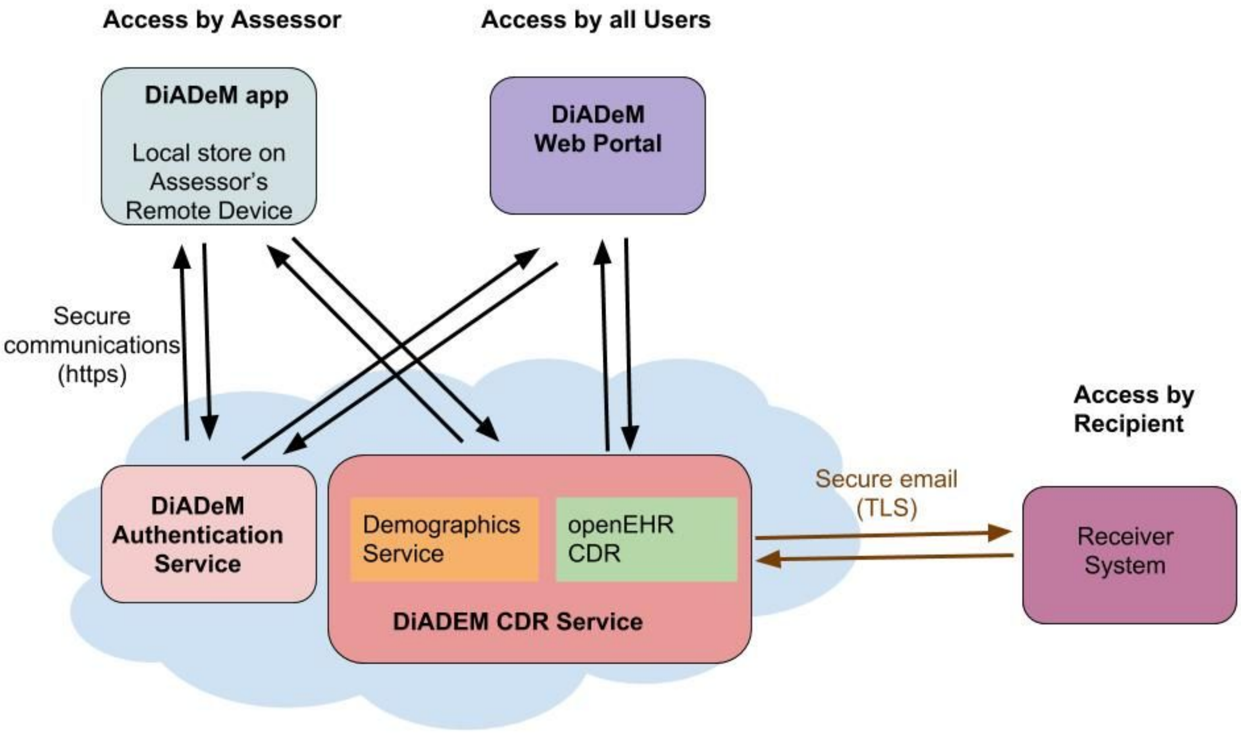
The **non-clinical Auditor** is a **User Role**. The **non-clinical Auditor** is able to access reporting information from the **DiADeM Service**. This reporting information does NOT include any **Personal Data**.

5.6. inidus

inidus provides the IT cloud platform for the **DiADeM Authentication Service** and the **DiADeM CDR Service**.

6. Service Architecture

6.1. Schematic of System Architecture



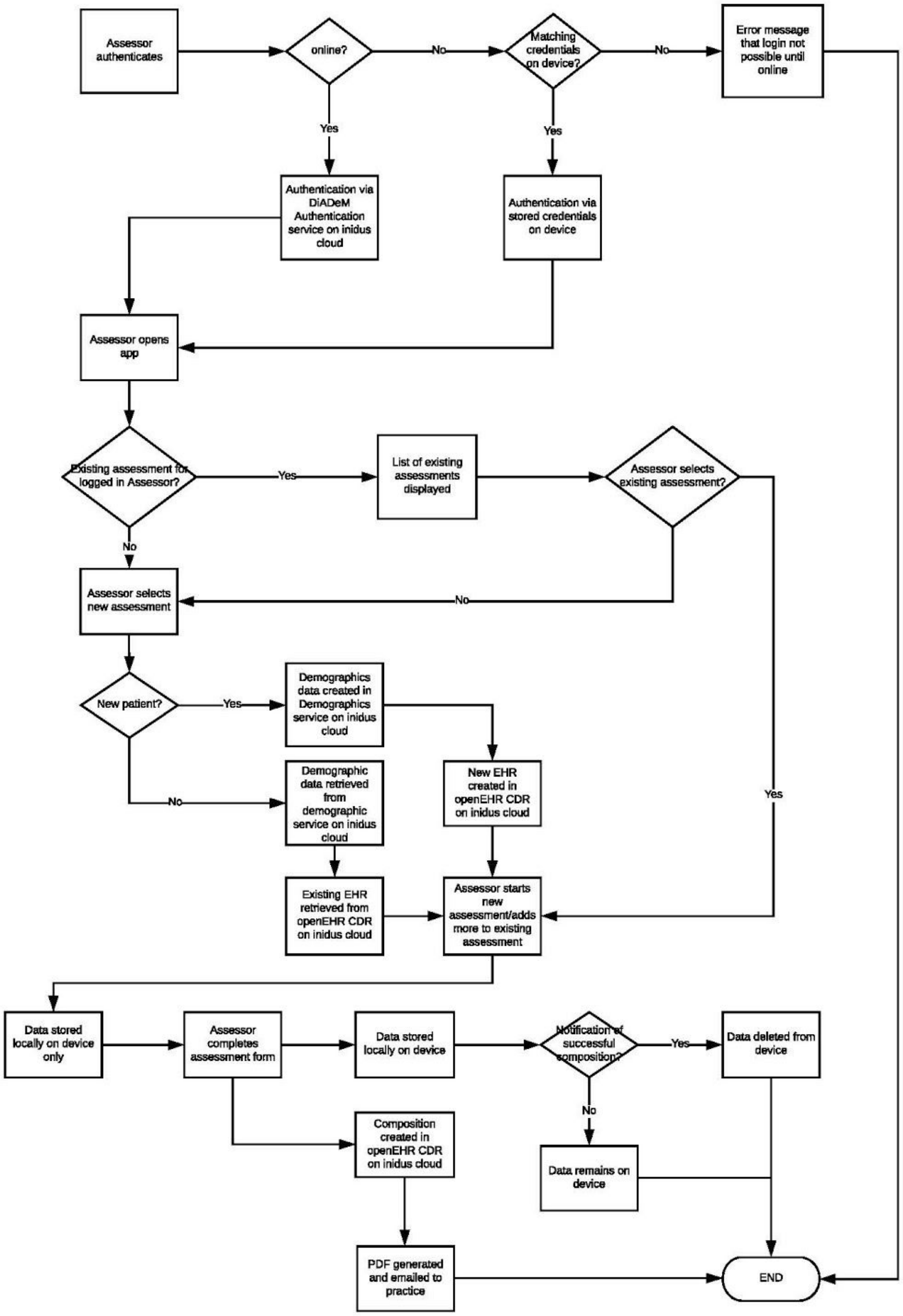
The schematic shows the different components of the **DiADeM Service**. The service comprises:

1. **DiADeM Authentication Service -** this stores access credentials of **User**s. This does NOT hold any patient **Personal Data**.
2. **DiADeM CDR Service**. This comprises a Demographics Service and openEHR CDR. The **DiADeM CDR Service** holds patient **Personal Data**.
3. **DiADeM app**. This is an that sits on the **Assessor**'s remote device, and is the tool that the **Assessor** uses to carry out a **DiADeM Assessment**
4. **DiADeM Web Portal**. This is used by all **User**s to register on the **DiADeM Service**, to manage their **DiADeM** account and and to carry out other **DiADeM Service** activities.

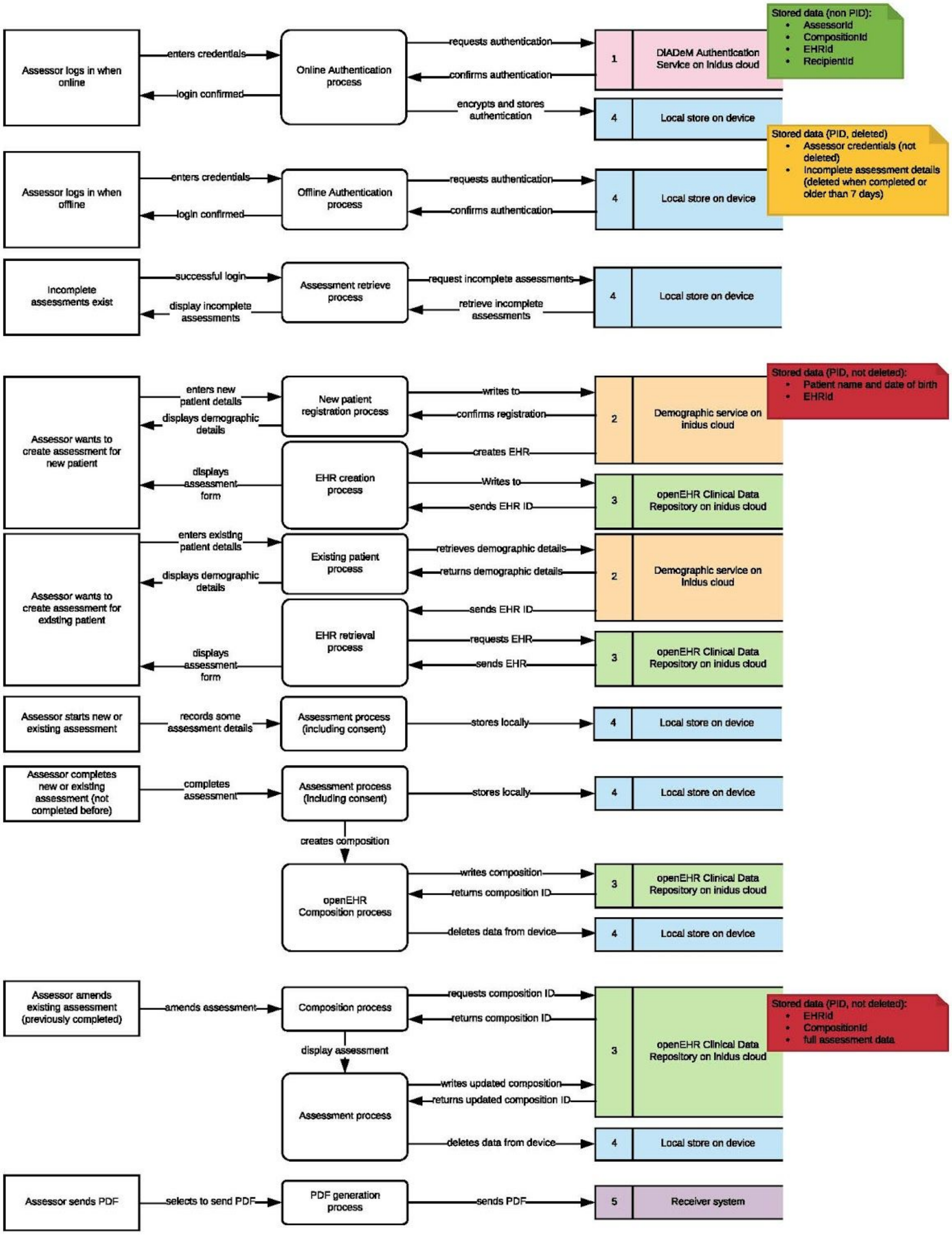
The **DiADeM CDR Service** emails the **DiADeM Assessment Report**s to the Receiver System where the **Recipient** receives it. The is emailed by securely using TLS encrypted communication, using nhs.net-to-nhs.net addressing: the **DiADeM CDR Service** uses an nhs.net domain email address and the **Recipient** is also required to use an nhs.net domain email address for receipt of the report.

The communication of all data in transit between remote systems and the cloud services uses secure https protocol.

6.2. Decision Process


Assessor authenticates
online?
No
Matching credentials on device?
No
Error message that login not possible until online
Yes
Yes
Authentication via DiADeM Authentication service on inidus cloud
Authentication via stored credentials on device
Assessor opens app
Existing assessment for logged in Assessor?
Yes
List of existing assessments displayed
Assessor selects existing assessment?
No
Assessor selects new assessment
No
New patient?
Yes
Demographics data created in Demographics service on inidus cloud
No
Demographic data retrieved from demographic service on inidus cloud
New EHR created in openEHR CDR on inidus cloud
Yes
Existing EHR retrieved from openEHR CDR on inidus cloud
Assessor starts new assessment/adds more to existing assessment
Data stored locally on device only
Assessor completes assessment form
Data stored locally on device
Notification of successful composition?
Yes
Data deleted from device
No
Composition created in openEHR CDR on inidus cloud
Data remains on device
PDF generated and emailed to practice
END

6.3. Data Flows


Assessor logs in when online
enters credentials
login confirmed
Online Authentication process
requests authentication
confirms authentication
encrypts and stores authentication
1
DIADeM Authentication Service on Inidus cloud
Stored data (non PID):
• AssessorId
• CompositionId
• EHRId
• RecipientId
4
Local store on device
Stored data (PID, deleted)
• Assessor credentials (not deleted)
• Incomplete assessment details (deleted when completed or older than 7 days)
Assessor logs in when offline
enters credentials
login confirmed
Offline Authentication process
requests authentication
confirms authentication
4
Local store on device
Incomplete assessments exist
successful login
display incomplete assessments
Assessment retrieve process
request incomplete assessments
retrieve incomplete assessments
4
Local store on device
Assessor wants to create assessment for new patient
enters new patient details
displays demographic details
New patient registration process
writes to
confirms registration
2
Demographic service on inidus cloud
Stored data (PID, not deleted):
• Patient name and date of birth
• EHRId
creates EHR
displays assessment form
EHR creation process
Writes to
sends EHR ID
3
openEHR Clinical Data Repository on inidus cloud
Assessor wants to create assessment for existing patient
enters existing patient details
displays demographic details
Existing patient process
retrieves demographic details
returns demographic details
2
Demographic service on inidus cloud
sends EHR ID
displays assessment form
EHR retrieval process
requests EHR
sends EHR
3
openEHR Clinical Data Repository on inidus cloud
Assessor starts new or existing assessment
records some assessment details
Assessment process (including consent)
stores locally
4
Local store on device
Assessor completes new or existing assessment (not completed before)
completes assessment
Assessment process (including consent)
stores locally
4
Local store on device
creates composition
openEHR Composition process
writes composition
returns composition ID
3
openEHR Clinical Data Repository on inidus cloud
deletes data from device
4
Local store on device
Assessor amends existing assessment (previously completed)
amends assessment
Composition process
requests composition ID
returns composition ID
display assessment
Assessment process
writes updated composition
returns updated composition ID
3
openEHR Clinical Data Repository on inidus cloud
Stored data (PID, not deleted):
• EHRId
• CompositionId
• full assessment data
deletes data from device
4
Local store on device
Assessor sends PDF
selects to send PDF
PDF generation process
sends PDF
5
Receiver system

7. **Data Controller** and **Data Processor**

1. **Apperta** is the **Data Controller** of data held on the **DiADeM Authentication Service**.
2. The **Assessor** (or the organisation under which they carry out the **DiADeM Assessment**) is the **Data Controller** for all **DiADeM** patient data collected by the **Assessor** that resides on the **DiADeM CDR Service** or on the **Assessor**'s remote device.
   Where the **Assessor** emails the **DiADeM Assessment Report** to the **Recipient**, the **Assessor** relinques their **Data Controller** responsibility of that patient's **DiADeM Personal Data**. In all cases, the **Assessor** may hold and have control of the patient **DiADeM** for a maximum of 7 days, after which the data is deleted or otherwise becomes non-accessible to the **Assessor**.
3. The **Recipient**'s organisation is the **Data Controller** for the **DiADeM Assessment Report** that they receive from the **Assessor**. The **Recipient's** organisation is required to hold the report according to the **Recipient** organisation's existing data policies and procedures.
   The **Recipient** becomes the **Data Controller** for the **DiADeM** patient data at the moment that the **Recipient** receives the **DiADeM Assessment Report** by email.
4. **inidus** is the **Data Processor** for the **DiADeM Authentication Service** and the **DiADeM CDR Service**.

8. Information Governance and Security

The **DiADeM Service** is operated in accordance with current statutory regulations concerning information governance.

A **Privacy Impact Assessment (PIA)** has been undertaken specifically concerning the duty of care of patient data. This **PIA** may be downloaded from the **DiADeM Web Portal**.

There is a **Retention Period** for all **DiADeM** data that the **Assessor** collects. This **Retention Period** is measured from the time and date when the patient's data was first saved by the **Assessor**. The **Retention Period** is 7 days, and at the end of 7 days, all data relating to the patient are automatically deleted from the systems.

Where data is held by the **DiADeM app** on the **User**'s remote device, there is a possibility that data may remain on the device longer than the defined **Retention Period**. For example, the **User** may not switch the remote device on**.** A number of measures are in place to prevent access to the data at ANY time after the expiry of the **Retention Period.** Furthermore, the data will be physically deleted from the device the next time the **User** opens the **DiADeM app**. The **User** is unable to prevent automated deletion of the data.

All data in transit is encrypted. The **DiADeM Service** emails any **Personal Data** of the patient using nhs.net-to-nhs.net addressing and TLS encrypted communication.

The **DiADeM Service** is operated with comprehensive cyber security measures in place in accordance with **Apperta**'s Security Policy. The measures include full encryption of **Personal Data** and passwords on the remote device.

9. **User** Terms and Conditions

All **User**s are required prior to their use of the **DiADeM Service** to sign-up to the **DiADeM** Terms and Conditions. This is done by the **User** online, via the **DiADeM Web Portal**.

10. Component Services and Tools

This section describes the component services and tools of the **DiADeM Service.**

The **DiADeM Service** comprises the following components:

1. **DiADeM Authentication Service**
2. **DiADeM CDR Service**
3. **DiADeM Web Service Tools**

Each of these are described below.

10.1. **DiADeM Authentication Service**

The Authentication Service holds **User** information for the purposes of managing permitted access and sharing of information held by the **DiADeM Service**.

The **DiADeM Authentication Service** holds the following data types only:

1. **User Personal Data** as required to authorise the **User**'s use of the **DiADeM Service**
2. **CompositionID**
3. **ehrID**

Items 2 and 3 are identifiers relating to the patient. They do NOT in themselves provide any ready identification of the patient or the patient's **Personal Data**. The **DiADeM Authentication Service** holds no other data that has any relationship to the patient.

The only way that the patient may be identified with these identifiers is to combine them with information held on the **DiADeM CDR Service**. This service is held separately from the **DiADeM Authentication Service**. Both services are controlled by robust information governance procedures.

For these reasons, we consider that the **DiADeM Authentication Service** does NOT hold any patient **Personal Data**. The ONLY **Personal Data** held on the **DiADeM Authentication Service** is that of the **User**s.

10.2. **DiADeM CDR Service**

The **DiADeM CDR Service** holds data that is collected by the **DiADeM Assessment** of each patient. It contains patient **Personal Data**.

10.3. **DiADeM** Web Service Tools

The **DiADeM** Web Service Tools comprise the following components:

1. **DiADeM Web Portal**
2. **DiADeM app**

The **DiADeM Web Portal** enables the **User** to self-manage their **DiADeM** account and to access help and support

The **DiADeM app** is an app that **User**'s with the role of **Assessor** can use to carry out a **DiADeM Assessment** of a patient. The app is presently available for IOS and Android, and may be downloaded from Apple iTunes and the Google Play Store. The **Assessor** is required to download the app and use it on their remote device prior to undertaking a **DiADeM Assessment**.