IT Services Agreement

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-assessm

	ents/)
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. Parties in the agreement

1. **Apperta**

2. **inidus**

4. Subject Matter

1. This agreement is concerned with the **DiADeM Service**, which is a clinical tool to assess moderate onset dementia. The details of the **DiADeM Service** are provided at the link.

2. The agreements listed on the table below are relevant to this **Agreement [2]**.

3. **Agreement [4]** is subordinate to this **Agreement [2]**.

4. This **Agreement [2]** permits Apperta to re-assign **Agreement [5]**.

Title of Agreement	**Abbreviation**	**Parties of agreement**
IT Services Agreement	**Agreement [2]**	Apperta, inidus
Data Processing Agreement: Apperta-inidus	**Agreement [4]**	Apperta, inidus
Data Processing Agreement: User-inidus	**Agreement [5]**	User, inidus

5. Purpose of Agreement

1. The purpose of the agreement is the provision of **IT Services** for the **DiADeM Services** by **inidus**.

6. Duration

1. The duration of this **Agreement [2]** is indefinite.

7. Notice

1. Either Party may serve notice at any time by issuing a “Notice of IT Services termination” to the other party.

2. **Apperta** and **inidus** agree that the notice period for termination of **IT Services** is three complete calendar months.

8. Supply

Inidus agrees to deliver **IT Services** as detailed under the contracts:

1. **Agreement [2]**; and
2. **Agreement [4]**.

8. End of Contract Provision

Where a “Notice of IT Services termination” has been served:

1. **inidus** will assist and fully cooperate with **Apperta** to transfer the IT Services to another IT provider;

2. Where there are no **registered Users** for the **DiADeM Service**, then **inidus** will assist and fully cooperate with **Apperta** to close down the **DiADeM Service** in regards to the **IT Services;**

3. **Inidus** agrees to re-assign the **Agreement [5]** to another party determined by Apperta;

4. Where **Agreement [5]** is reassigned, **inidus** discharges all future liabilities concerning **Agreement [5]**;

5. **Apperta** agrees to reimburse **inidus** reasonable costs that may be incurred by **inidus** to provide the required support;

6. At the end of the notice period:
    a. **Apperta** will instruct **inidus** to delete all **DataDD** for which **Apperta** is the **Data Controller**;
    b. **inidus** is permitted to freely delete any data that remains on IT systems that remain under the control of **inidus** on cessation of this contract, and that **inidus** had used to deliver IT Services for DiADeM: **inidus** understands that all **Data Controllers** will have had sufficient time to remove their data;

7. On completion of the notice period, the following agreements terminate:
    a. **Agreement [2]** -- IT Services Agreement; and
    b. **Agreement [4]** -- Data Processing Agreement: Apperta-inidus.

9. Obligations and Rights of the Data Controller

1. **Apperta** shall act in full accordance with its duties as **Data Controller** for **DataDD** held on the **DiADeM Authentication Service**.

2. Apperta shall strictly abide by its obligations and rights as detailed in the **Agreement [4]**, which is subordinate to this **Agreement [2]**.

3. **Apperta** shall handle **DataDC** in strict compliance with the prevailing data protection legislation applicable to the UK.

4. Nothing in this agreement relieves the **Data Controller** of its own direct responsibilities and liabilities under the prevailing data protection legislation applicable to the UK..

10. Obligations and Rights of the Data Processor

1. **inidus** shall act in full accordance with its duties as **Data Processor** for **DataDD** held on the **DiADeM Service.**

2. Inidus shall strictly abide by its obligations and rights as detailed in the **Agreement [4]** which is subordinate to this **Agreement [2]**.

3. **inidus** shall handle **DataDC** in strict compliance with the prevailing data protection legislation applicable to the UK.

4. Nothing in this agreement relieves the **Data Processor** of its own direct responsibilities and liabilities under the prevailing data protection legislation applicable to the UK.