DiADeM Service Use Agreement: Apperta - User

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. Parties in the agreement

1. User
2. Apperta

4. Subject Matter

1. The agreement concerns the **DiADeM Service**. This is a cloud delivered software as a service, with supporting web tools and apps.

2. The **DiADeM Service** is a clinical tool to assess moderate onset dementia.

3. The details of the **DiADeM Service** are provided at the link.

4. The agreements listed on the table below are relevant to this **Agreement [3]**.

5. This **Agreement [3]** is subordinate to the **Agreement [1]**.
6.
7. Agreement [5] is referred to as the form of agreement required as to be in placed with the **Data Processor**.

Title of Agreement	**Abbreviation**
DiADeM Service User Agreement: Main	**Agreement [1]**
DiADeM Service Use Agreement: Apperta-User	**Agreement [3]**
Data Processing Agreement: User - inidus	**Agreement [5]**

5. Agreement

5.1. Duration

1. This **Agreement [3]** is continuous whilst the **User** is a registered **User** of the **DiADeM Service**.

2. This **Agreement [3]** ceases when the **User** is no longer a registered **User**.

5.2. Notice

1. Notice may be served by the superior **Agreement [1]** issuing a “Notice of termination of DiADeM Service Registration”.

2. Where Notice is served, then the notice period of this **Agreement [3]** is the same as **Agreement [1]**.

5.3. End of Contract Provision

1. The end of contract provisions are as detailed in the superior **Agreement [1]**.

6. Nature and Purpose of Agreement

1. The purpose of the Agreement are the terms and conditions by which **Apperta** supplies the **DiADeM Service** to the **User**.

2. The agreement is limited to the supply of the **DiADeM Service** by **Apperta**, and the use of the **DiADeM Service** by the **User**.

3. Under this agreement:

    a. **Apperta** is the **Data Controller** for **Personal Data** provided by the **User** and held on the **DiADeM Authentication Service**; and

    b. The **Data Subjects** for which **Apperta** is the **Data Controller** are the **Users** who have registered to use the **DiADeM Service**.

    c. Certain roles of **User** (or **User’s** organisation) agree to be the **Data Controller** for **Personal Data** held on the **DiADeM CDR Service**.

7. Types of Personal Data and Categories of Data Subject

1. The types of **Personal Data** covered by this agreement are **Personal Data** of the **User**, where the **User** is the **Data Subject**:

a. Name
b. Contact details
c. Organisation for whom the **User** is undertaking working concerning **DiADeM**
d. Organisations with which the **User** is associated within a professional capacity, and which has interests in the **User**'s work concerning **DiADeM**.

2. The categories of **Data Subject**s are **Users** who register to use the **DiADeM Service**.

3. The categories of **Data Subject** covered under this agreement does NOT include patients.

8. User's Instructions to Apperta

1. For any **User** who is a **Data Controller** of **DataDD** held by the **DiADeM CDR Service**, the **User** instructs **Apperta** that **Apperta** is permitted and required to provide the following **User**'s **DataDD** to the **DPcdr,** which is held on the **DiADeM Authentication Service**:

    a. The Name of the **User**;
    b. The contact details of the **User**; and
    c. The **EHRIDs** for all **DataDD** for which the **User** is the **Data Controller**.

    In the foregoing, items (a) and (b) are the **Personal Data** of the **User**, and item (c) does not constitute **Personal Data** in its form held on the **DiADeM Authentication Service**.

2. The **User** instructs **Apperta** that the disclosure of this **DataDD** to the **DPcdr** is for the sole purpose: To enable the **DPcdr** to discharge the **DPcdr**'s obligations as **Data Processor** of the **DiADeM CDR Server**.

3. **Apperta** agrees to deliver to the **DPcdr** in a timely and prompt manner, the information detailed in clause (1) and regular updates, if and whenever there are changes to the information.

4. Where any **User** who ceases to be the **Data Controller** of any **DataDD** held by the **DiADeM CDR Service**, **Apperta** agrees to instruct the **DPcdr** to delete all **Subject Data** of the **User** that the **DPcdr** holds for the **Data Subject** that has been provided to the **DPcdr** under this **Agreement [3]**.

9. Obligations and Rights of Apperta

9.1. Compliance with applicable laws and regulations

1. **Apperta** shall act in full accordance with its duties as **Data Controller** for all **Personal Data** covered by this agreement and detailed in the section above “Types of Personal Data and Categories of Data Subject”**.**
2. **Apperta** shall handle **DataDC** in strict compliance with the prevailing data protection legislation applicable to the UK.
3. Nothing in this agreement relieves the **Apperta** of its own direct responsibilities and liabilities under **GDPR**.

9.2. Delivery of DiADeM Service

1. **Apperta** will act as the the administrator of the **DiADeM Service.**

2. **Apperta** will deliver and suitably maintain for clinical purposes, the **DiADeM Web Service Tools**, which includes the **DiADeM web portal** and the **DiADeM app**.

3. **Apperta** will make available to the **User** the **DiADeM Web Service Tools** according to the **User**’s registered **User Role**.

4. Where the **User**’s role requires **Access** to the **DiADeM CDR Service, Apperta** will enable the **User** to have secure **Access** to this **DiADeM CDR Service** using the **DiADeM Web Service Tools**.

5. **Apperta** will include within the **DiADeM Web Service Tools**, the following capabilities, for the purposes of enabling a **User** to manage all **DataDD** for which the **User** is the **Data Controller**:
    a. Delete all or part**;**
    b. Deliver to the **User** in a machine readable, open standard format; and
    c. Transfer the **Data Controller** responsibilities to another **User** registered on the **DiADeM Service**, providing this other **User** is suitably registered on the **DiADeM Service** and has a legitimate purpose to be the **Data Controller** for **DataDD**.

6. **Apperta** will make all reasonable efforts to ensure that all tools operate correctly.

7. **Apperta** will maintain the operation of the **Web Service Tools** to be compliant with the security principles in Article 32 of **GDPR**.

8. **Apperta** will maintain the operation of the **Web Service Tools** to be compliant with the "Data Protection by Design and by Default" principles (Article 25, **GDPR**), as far as is reasonably practicable.

9.3. Appointment of Data Processors: GDPR compliance and protecting rights of data subjects

1. In delivering the **DiADeM Service**, **Apperta** will a **Data Processor** to undertake data processing of the **DiADeM Service DataDD**.

2. Apperta shall ensure that the **Data Processor** provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of **GDPR** and prevailing data protection legislation applicable to the UK, and ensure the protection of the rights of the **Data Subject**

3. **Apperta** will ensure that all data processing that **Apperta** contracts to third parties, is contractually agreed under a Data Processing Agreement with the **Data Processor**, where the Data Processing Agreement is compliant with Article 28.3 of the **GDPR** and prevailing data protection legislation applicable to the UK. In this way, the Data Processing Agreement will protect the rights of all data subjects whose **Personal Data** is held by the **DiADeM Service**.

4. **Apperta** will hold regular review meetings with the **Data Processor** which will include:

    a. Risk Assessment: review of information governance and other issues concerning **GDPR**; and
    b. Agreed actions to mitigate or reduce identified risks where appropriate.

9.4. Data Protection Policy

1. **Apperta** will maintain a Security Policy that is compliant with **Apperta**'s obligations under **GDPR** and the prevailing data protection legislation applicable to the UK.

9.5. Records

9.5.1. Processing Activities

Apperta will maintain the following records for all **DataDC** for which **Apperta** is the **Data Controller**:

1. Purpose of the processing;
2. Name and contact details of the data processor, and all standing instructions;
3. Categories of the Data Subjects and of Personal Data held by Apperta;
4. Categories of recipients to whom **Apperta** discloses any **Personal Data**;
5. Name of any third countries or international organisations to whom Apperta transfers personal data; and
6. Where possible, the envisaged time limits for erasure of the different categories of data.

9.5.2. Technical and Organisational Measures

1. Apperta will maintain documentation for the DiADeM Service that provide a general description of the technical and organisational security measures referred to in **GDPR** Article 32(1).

9.6. DiADeM Service Performance

1. **Apperta** aims to offer the **Data Service** with an uptime of 99% (excluding scheduled maintenance) in any calendar month.

2. Where **Apperta** fails to meet this uptime, **Apperta** will waive all charges for that calendar month period.

3. Scheduled maintenance will occur between 0200 and 0400 daily

9.7. Privacy Notice- Apperta

1. **Apperta** will provide a template Privacy Notice for use by **Assessor**, for the purposes of enabling the **Assessor** to inform the patient and their carers as appropriate, how the patient's **Personal Data** that is collected during the **DiADeM Assessment** will be used and who will be the **Data Controller** of the patient's **Personal Data**.

9.8. Governance

1. **Apperta** shall maintain a Security Policy that is compliant with GDPR and the prevalent UK legislative data regulations concerning security of sensitive PID.
2. **Apperta** will manage all **Personal Data** for which **Apperta** is responsible within the role of **Data Controller**, in strict accordance with the **Apperta** Security Policy.
3. **Apperta** will ensure that the tools that **Apperta** offers as part of the of the **DiADeM Service** will manage **Personal Data** in strict accordance with the **Apperta** Security Policy.

9.9. Data Retention

1. **Apperta** will delete all **User Personal Data** when the **User** ceases to be a registered **User** of the the **DiADeM Service**.

9.10. Management of the User's Access Permissions

Apperta will ensure that the **User**'s access permissions to **Data** is:

1. Maintained to be appropriate at all times for the **User**'s role.

9.11. Breach of Personal Data - Apperta

In all cases where there is a **Breach** or suspected **Breach of Personal Data** for which **Apperta** holds the responsibility of **Data Controller**, **Apperta** will**:**

1. Record:
    a. All **Breach**es even if they do not need to be reported;
    b. The facts relating to the breach, its effects and remedial action taken.
2. Assess the likely risk to the rights and freedoms of individuals as a result of a breach as detailed under Section IV of the Article 29 **GDPR** Working Party;
3. Notify the **ICO** of the **Breach** (in their capacity as the lead supervisory authority) without undue delay but not later than 72 hours of becoming aware of the **Breach** where the risk assessment indicates a potential risk to the rights and freedoms of the individual;
4. Where the risk assessment indicates a potential HIGH risk to the rights and freedoms of the individual notify the individual of the **Breach** without undue delay.
5. Investigate whether the **Breach** was a result of human error or a systematic issue and establish how a recurrence can be prevented.

9.12. Security

1. **Apperta** will operate according to the **Apperta** Security Policy and Standard Operating Procedures that are compliant with the prevalent legislative data regulations concerning security of **Personal Data** and Article 32 of the GDPR.
2. **Apperta** will deliver the appropriate level of security through implementing technical and organisational measures
3. **Apperta** will determine the appropriate level of security through undertaking risk assessment (as defined within **Apperta**'s Security Policy and Standard Operating Procedures).
4. **Apperta** shall ensure that all software tools that **Apperta** supplies to the **User** as part of the **DiADeM Service** will have in place all reasonable and appropriate security measures.
5. **Apperta** will maintain necessary security systems to be up-to-date.

9.13. Control of Access to Apperta Data and Systems

1. **Apperta** will restrict **Access** of **Apperta Data and Systems** exclusively to **Apperta Personnel** only, a single exception all registered **User**s have permitted **Access** via the **DiADeM Web Service Tools** solely for the purpose defined by their registered role.

2. **Apperta** will comply with the following principles for permitting **Access** by **Apperta Personnel** to **Apperta Data and Systems**:

    a. All **Access** is avoided whenever this is practical;
    b. All **access** is authorised by a designated **Apperta** manager; and
    c. Only authorised persons are permitted to have **Access**.

3. **Apperta** will regularly review **Access** permissions and the purpose for **Access**. **Apperta** will make necessary changes to permissions commensurate with the purpose.

4. **Apperta** will maintain records of all permissions that it grants for **Access** to **Apperta Data and Systems**. The records will include:

    a. Name,
    b. Organisation
    c. Contact details; and
    d. Purpose for access**.**

5. **Apperta** will take the following actions if there is unauthorised **Access** by **Apperta Personnel** to the **Apperta IT Systems**:

    a. Compliance with the conditions outlined in the section entitled “Breach of Personal Data - Apperta” within this agreement where there is a breach or possible breach of personal data.

    b. Where there is any intentional **Access:**
        i. **Apperta** will summarily dismiss the **Apperta Personnel**.
        ii. **Apperta** will consider further action that includes prosecution and notification to any relevant professional body for possible disciplinary action.

    c. Where there is any unintentional **Access:**
        i. The **Apperta Personnel** are required to report the incident to the **Apperta** management at the earliest opportunity.
        ii. The **Apperta** management will carry out an investigation to determine if the circumstance of the unintentional access justifies disciplinary action.

    d. Record of event and actions taken.

9.14. Data Subject’s rights

1. **Apperta** will provide tools and assistance to fully support the **Data Subject**’s rights to their data held on the **DiADeM Service**, where the **Data Subject**’s rights are as defined in the prevalent data protection legislation applicable to the UK.

9.15. Backup

1. **Apperta** stores all data for which it holds responsibility as **Data Controller** on fault tolerant systems making data loss caused by failure of the **Apperta DiADeM Service** an unlikely event. **Apperta** makes regular backups of the data stored by the **DiADeM Service**.
2. In the event of data loss resulting from a service failure, **Apperta** will restore the data to the point of the most recent backup.

10. Obligations and Rights of All Users

10.1. Compliance with all applicable laws and regulations

1. The User agrees to use the DiADeM Service for only holding Data that the User may lawfully hold.

2. The User, in their use of the DiADeM Service, will act in strict compliance with the prevailing data protection legislation applicable to the UK.

3. Nothing in this agreement relieves the **User** of its own direct responsibilities and liabilities under **GDPR**.

10.2. Authority

1. The **User** confirms that they have authority to sign-up to this agreement.

10.3. Accurate information

1. The **User** agrees to maintain all **User** registration information up-to-date.

10.4. Appointment of Data Processors: GDPR compliance and protecting rights of data subjects

1. For any **User** that uses a **Data Processor** as part of the **DiADeM Service**, and where the **User** has the responsibility of **Data Controller** for **DataDD**, then the **User** shall use the form of the **Agreement [5]** as the contractual undertakings of and relationship with the **Data Processor**.

2. The **User** understands that the **Agreement [5]** will meet the requirements of **GDPR** and prevailing data protection legislation applicable to the UK, and ensure the protection of the rights of the **Data Subject**

10.5. Documented Instructions

1. The **User** understands that, where they or their organisation act in the capacity as **Data Controller** of **DataDD held on the DiADeM CDR Service**, that the **User** or their organisation will be the only party who issues instructions to the **Data Processor**.

10.6. Demonstrating Compliance with prevailing data protection legislation applicable to the UK

1. The **User** understands that **Apperta**, through their provision of the **DiaDeM Service**, will provide compliance with prevailing data protection legislation applicable to the UK for all **DataDD** that is managed by the **DiADeM Service**

2. The clause does not relieve the **User** of their own responsibilities:

    a. For ensuring that at all times they adopt good practice;
    b. Ensuring that all data entered into the system is properly acquired and legally held; and
    c. For any data which is released beyond the control of the **DiADeM Service**.

10.7. Sharing and Copying Personal Data

The **User** agrees to comply with the following measures:

1. The **User** will share **Personal Data** with others in compliance with applicable laws and regulations ; and

2. The **User** will ensure that information that they access via the **DiADeM Service** is recorded elsewhere only in compliance with applicable laws and regulations.

10.8. Data Retention

1. All **User**'s shall comply strictly with the **Data Retention Period**.
2. The **User** will ensure that, the **Personal Data** relating to **DiADeM Assessments** that they have access to or are otherwise responsible, are safely and permanently deleted outside this time period.

10.9. Breach of Personal Data - All Users

The **User** will appoint a responsible person with the responsibility for managing **Breaches of Personal Data** for which the **User** holds responsibility as **Data Controller**.

In all cases where there is a **Breach** or suspected **Breach of Personal Data** for which the **User** is the **Data Controller**, the **User** will**:**

1. Record:
    a. All **Breach**es even if they do not need to be reported;
    b. The facts relating to the breach, its effects and remedial action taken.
2. Assess the likely risk to the rights and freedoms of individuals as a result of a breach as detailed under Section IV of the Article 29 **GDPR** Working Party;
3. Notify the **ICO** of the **Breach** (in their capacity as the lead supervisory authority) without undue delay but not later than 72 hours of becoming aware of the **Breach** where the risk assessment indicates a potential risk to the rights and freedoms of the individual;
4. Where the risk assessment indicates a potential HIGH risk to the rights and freedoms of the individual, notify the individual of the **Breach** without undue delay.
5. Investigate whether the **Breach** was a result of human error or a systematic issue and establish how a recurrence can be prevented.

10.10. Secure Operation

1. The **User** agrees to take all reasonable precautions to prevent theft and keep safe:

    a. All **Sensitive Data**;
    b. All passwords and access credentials to the **DiADeM Service** (including not divulging these to other persons)**;** and
    c. All physical devices owned or used by the **User** that hold the **DiADeM app** and any **Personal Data** or other data relating to the **DiADeM Service**.

2. The **User** agrees to take all reasonable cybersecurity measures on any device that they use to access the **DiADeM Service**. This includes:

    a. Use of anti-virus software and keeping this up-to-date; and
    b. Ensuring that system updates are applied to their computer systems and networks from which the **User** accesses the **DiADeM Service**.

3. In the event of loss or compromise of passwords or access credentials for the **DiADeM Service,** the **User** agrees to change their access credentials (includes passwords) that may have been compromised at the earliest opportunity, and notify the **Data Controller**

if there is any possibility that there has been unauthorised access to any part of the **DiADeM Service**.

4. In the event where there is suspected or actual cyber security incident on a device that the **User** uses to access the **DiADeM Service,** the **User** agrees to:

    a. Stop usage of the **DiADeM Service** with immediate effect;
    b. Notify the **Data Controller** of the incident;
    c. Notify **Apperta** or otherwise ensure that access credentials are suitably changed so as to prevent unauthorised access;
    d. Decontaminate their device; and
    e. Ensure that the device is fully decontaminated prior to accessing the **DiADeM Service again** using their device.

11. Obligations and Rights of Assessors

This section is only for **User**s who are registered as **Assessors**.

11.1. Data Controller

1. Where the **User** is registered in their capacity as an employee, partner or agent (their "organisation") for whom they are undertaking work concerned with **DiADeM:**

    a. The **User confirms that** their organisation is registered with the **Information Commissioner's Office (ICO)** and will maintain the registration up to date; and
    b. The **User** agrees that their organisation will take full responsibility as the **Data Controller** for all **person identifiable data (PID)** collected by the **DiADeM Service**, including meeting all legal obligations as per relevant legislative and regulatory requirements.

2. Where the **User** is registered in their capacity as a sole trader including operating under a business name which is not a legal entity:

    a. The **User** confirms that they are registered with the **ICO** and will maintain the registration up to date; and
    b. The **User** agrees that they will take full responsibility as the **Data Controller** for all **PID** collected by the **DiADeM Service**, including meeting all legal obligations as per relevant legislative and regulatory requirements.

3. Where the Assessor has sent a completed **DiADeM Assessment** to a **Recipient**, the **User (**or the organisation under which the **User** carries out the **DiADeM Assessment**) ceases to be the Data Controller for any patient **DiADeM Assessment** that they have collected at the moment that the report is received by the **Recipient**.

11.2. Data Retention

1. The **Retention Period** for **DiADeM Assessment Data** collected by the **Assessor** for each patient, is 7 days, measured from the time that the **Assessor** first started to carry out the **DiADeM Assessment** of the patient.

11.3. Transmission of DiADeM Assessment Report

1. The **User** agrees to transmit **DiADeM Assessment Reports** and any personal data collected as part of the DiADeM Assessment conducted using the **DiADeM Service,** using only the services provided by the **DiADeM Service**.

2. The **User** is responsible for ensuring that they select the correct **Recipient** for the receipt of the **DiADeM Assessment Report.**

3. Following submission of a completed **DiADeM Assessment Report**, the **User** will receive a submission report in the form of an email from the **DiADeM Service**. This report will provide confirmation that the **DiADeM Assessment Report** has been submitted, and the name of the **Recipient**. The **User** should use this report to check that they have selected the correct **Recipient** to receive the **DiADeM Assessment Report**.

11.4. Dispatch of the DiADeM Assessment Report to the wrong Recipient

1. Where the **User** dispatches a **DiADeM Assessment Report** to the **Recipient,** the **User** accepts that it is the **User**'s full responsibility to select the correct **Recipient** for emailing each completed **DiADeM Assessment Report**.

2. The **User** accepts that **Apperta** cannot not be held liable for any consequences following dispatch of the **DiADeM Assessment Report** to the wrong Recipient, where causations may include:

a. The incorrect **Recipient** being selected by the **User**; or
b. The email mail service incorrectly routing the email due to errors of the mail service outside of **Apperta**'s control.

3. If, following dispatch of the **DiADeM Assessment Report** to a **Recipient**, the **Assessor** determines that they have selected the wrong **Recipient**, the **Assessor** will:

    a. Comply with the conditions outlined in the section entitled "Breach of Personal Data - All Users" within this agreement; and
    b. Re-enter the **DiADeM Assessment Data** and re-submit the **DiADeM Assessment Report** to the correct **Recipient**.

11.5. Qualification

The **User** confirms that they are:

1. Qualified to make the necessary decisions regarding the capacity of the patient to provide consent for the **DiADeM Assessment**; and

2. Appropriately qualified and trained to conduct the **DiADeM Assessment**, including avoiding causing distress to the patient.

11.6. Required Explanation of DiADeM assessment to Patient

The **User** agrees to explain to the patient prior to undertaking the **DiADeM Assessment**:

1. What the **DiADeM Assessment** is for and why the **User** will be taking the patient through the **DiADeM Assessment**;

2. That at the end of the **DiADeM Assessment** the patient may have a diagnosis of Moderately Advanced Dementia;

3. What the **DiADeM Assessment** may mean to the patient in terms of Care planning, help and support going forward;

4. All records will be shared and held safely by the GP or clinician responsible for the patient's long term care; and

5. The **Data** will held in accordance with the GP/ clinician's existing information sharing agreements, about which the patient has already been informed.

11.7. Privacy Notice

The **User** will provide:

1. A the template Privacy Notice provided by Apperta (refer to section “Privacy Notice-Apperta” within this agreement) to the patient and their carers as appropriate; and

2. Such assistance as may be practical to ensure the patient and their carers understand the privacy notice.

11.8. Patient Consent

Prior to undertaking the **DiADeM Assessment** of a patient:

1. The **User** agrees to establish, in accordance with the Mental Capacity Act 2005 and any other prevailing and applicable legislative regulations, that the patient has capacity to make ALL the following decisions:

    a. To undergo the **DiADeM Assessment**;
    b. To allow the **Assessor** to collect the patient’s personal data for the **DiADeM Assessment**; and
    c. To allow the clinician responsible for the patient’s long term care to see the **DiADeM Assessment Report**, and to retain it on the patient’s record.

2. Where the outcome of (1) above indicates that the patient does not have capacity, the **User** is required to established that it is in the patient’s best interest to undertake a **DiADeM Assessment**, and to share the **DiADeM Assessment Report**, which includes the patient’s **Personal Data**, with the clinician responsible for the long term care of the patient.

11.9. Identification of Patients

The **User** will ensure that a patient is always identified by use of ALL the following identifiers:

1. Patient’s Full Name (First Name/Surname);

2. Date of Birth; and
3. Location of care home at which the patient resides.

11.10. Permitted use of the DiaDeM app

1. The **User** is permitted to download the **DiADeM app** for use on their remote device, for the purpose of conducting the **DiADeM Assessment**.

2. This is the grant of a licence, not a transfer of title, and under this licence the **User** may not:

    a. Modify or copy the materials
    b. Use the materials for any commercial purpose, or for any public display (commercial or non-commercial);
    c. Attempt to decompile or reverse engineer any software contained within the **DiaDem app**;
    d. Remove any copyright or other proprietary notations from the materials; or
    e. Transfer the materials to another person or 'mirror' the materials on any other server.

3. This license shall automatically terminate if the **User** violates any of these restrictions and may be terminated by **Apperta** at any time. Upon terminating the **User**'s viewing of these materials or upon the termination of this license, the **User** must destroy any downloaded materials in the **User**'s possession whether in electronic or printed format.

4. The **User** agrees to delete the **DiADeM app** when they no longer have use of the **DiADeM Service** for their professional role.

12. Obligations and Rights of Recipients

This section is only for **User**s who are registered as **Recipients**.

12.1. Clinician with responsibility for long term care of patient

The **User** confirms that they are:

1. A clinician with responsibility for the long-term clinical care of patients; or

2. Acting as an employee, partner or agent for a clinician or clinician's organisation, where the clinician has responsibility for the long-term clinical care of the patients.

12.2. Data Controller

1. The **User** confirms that their organisation holds the responsibility as **Data Controller** and custodian of patients' **Personal Data** collected for their long term clinical care for patient data within their organisation. The **User** confirms that their organisation's policies and procedures are fully compliant with prevalent data protection legislation and regulations applicable to the UK.

2. The **User** agrees to handle all **Personal Data** received from the **DiADeM Service** according to the **User**'s organisation's data policies and procedures.

3. The **User** agrees that:

    a. Their local organisation will be the **Data Controller** for all data that originates from and is held by the **DiADeM Service** concerning the patient's **DiADeM Assessment** that has been sent to them by the **DiADeM Assessor**;
    b. The responsibility of **Data Controller** for the patient's **DiADeM Assessment Data** commences at the moment that the **User** receives the **DiADeM Assessment Report** from the **DiADeM Assessor**; and
    c. The **User**'s local organisation will hold all **Data** according to their local organisation's security and governance procedures concerning management of patient data.

12.3. Release of Data to other parties

1. Where the **User** receives a request for a copy of a **DiADeM Assessment Report**, where the stated purpose is regulatory compliance or legal necessity; and the request is by a person who had previously created the requested **DiADeM Assessment Report**; then the **User** is required to make this **DiADeM Assessment Report** available to the person requesting the report. In this case, the **User** will provide the information according to the **User**'s local security processes.

2. The **User** permits that all **Data** for which the **User**'s organisation is the **Data Controller** and which is held by the **DiADeM Service**, may be used by other **Users** of the **DiADeM Service** who have the following "**User** Registered Role" for the declared "Purpose" and where the "PID Content" is as stated:

a. **User** Registered Role: “non-clinical auditor”
   Purpose: Creation of Report
   PID Content: Fully anonymised information (no patient PID)

12.4. Data Retention

1. The retention period for DiADeM data held by the **User**’s organisation shall be in line with the **User**’s organisation’s information governance policy.

12.5. Expertise and Professionalism

1. The **User** confirms that they will bring to bear their professional expertise and clinical judgement on deciding how to act on the **DiADeM Assessment Report**, including seeking additional information and taking proportionate actions where they have issues or concerns on the quality or accuracy of the **DiADeM Assessment** that they have received.

12.6. NHS.NET email address

1. The **User** confirms that the nhs.net email address that they register on the **DiADeM Service** belongs to either the **User** or their organisation.

12.7. Receipt of DiADeM Assessment Report sent in error

1. The **User** confirms that where they receive a **DiADeM Assessment Report** that has been sent to them by email in error, that they will:

    a. Notify the **Assessor** that the email has been received in error, by replying to the received email; and
    b. Delete the received email.

13. Obligations and Rights of Non-Clinical Auditor

This section is only for **User**s who are registered as **Non-Clinical Auditor**.

13.1. Overview

1. A **User** registered as a non-clinical auditor may access and download reporting data from the **DiADeM Service**.

2. The purpose of the reports are to provide usage data of the **DiADeM Service**.

3. The reporting data is limited exclusively to **Data** that does NOT include **Personal Data** of any patient.

14. General Provisions

14.1. Indemnification

1. The **User** agrees to hold harmless and indemnify **Apperta**, and its, affiliates, officers, agents, employees, advertisers, licensors, suppliers or partners (collectively "**Apperta** and Partners") from and against any third party claim arising from or in any way related to (a) the **User**'s breach of the Terms, (b) the **User's** use of the **DiADeM Service**, or (c) the **User's** violation of applicable laws, rules or regulations in connection with the **DiADeM Service**, including any liability or expense arising from all claims, losses, damages (actual and consequential), suits, judgments, litigation costs and legal fees, of every kind and nature.

2. In such a case, **Apperta** will provide the **User** with written notice of such claim, suit or action, offer conduct of the claim to the **User** and provide reasonable assistance to the **User** (at the **User's** expense) to enable the **User** to defend such claims.

14.2. Other Content

1. The **DiADeM Service** may include hyperlinks to other websites or content or resources or email content. **Apperta** may have no control over any websites or resources which are provided by companies or persons other than **Apperta**.

2. The **User** acknowledges and agrees that **Apperta** is not responsible for the availability of any such external sites or resources, and does not endorse any advertising, products or other materials on or available from such websites or resources.

3. The **User** acknowledges and agree that **Apperta** is not liable for any loss or damage which may be incurred by the **User** or the **User's organisation** as a result of the availability of those external sites or resources, or as a result of any reliance placed by you on the completeness, accuracy or existence of any advertising, products or other materials on, or available from, such websites or resources.

14.3. Governing Law

1. This agreement shall be governed by the laws of England and Wales.

14.4. Force Majeure

1. In no event shall the Apperta be responsible or liable for any failure or delay in the performance of its obligations hereunder arising out of or caused by, directly or indirectly, forces beyond its control, including, without limitation, strikes, work stoppages, accidents, acts of war or terrorism, civil or military disturbances, nuclear or natural catastrophes or acts of God, and interruptions, loss or malfunctions of utilities, or communications; it being understood that the Apperta shall use reasonable efforts which are consistent with accepted practices within IT Services sector to resume performance as soon as.