

DATA PROTECTION PROTOCOL

Version 3

6 June 2023

NHS England – Midlands Region

Electronic Eye Care Referral System

PARTIES

- (1) MONMEDICAL LIMITED (t/a Cinapsis), with registered office address: Profile West Suite 2, First Floor, 950 Great West Road, Brentford, United Kingdom, TW8 9ES (Supplier), and
- (2) The Authority, as identified within the Agreement Signature Block, herein.

WHEREAS:

- (A) Monmedical Ltd., trading as Cinapsis, supplies a suite of software and services (the System) that supports clinician-to-clinician communications regarding patients under their direct care;
- (B) NHS England – Midlands Region Board (the Commissioners), have commissioned the use of the System, for Synchronus and Asynchronus Advice and Guidance Service;
- (C) The Authority has been nominated by the Commissioners, and accepts to use the System;
- (D) The Authority's nominated Users will use the System as part of communications with healthcare colleagues, in the provision of direct patient care;
- (E) The Authority, via its nominated Users, will enter Personal Data into the System and will do so acting as the Controller;
- (F) Cinapsis, at all times under the direction of the Controller, will be acting as the Processor of Personal Data;
- (G) In consideration of the fees paid to Cinapsis, under the Contract with the Commissioners, it agrees to enter into and comply with this Agreement which sets out the obligations as to how it will process personal information about patients or other service users, on behalf of the Authority and how it will comply with Data Protection Legislation.

Term and Termination

- (1) This Protocol shall come into force upon completion of the signature blocks herein, by the Parties, and will remain in force until terminated. It will terminate automatically:
 - a) upon written instruction by the Authority to Cinapsis, to effect termination, or
 - b) upon termination of the Contract entered into by the Commissioners and Supplier

Definitions

In this Protocol the following words shall have the following meanings unless the context requires otherwise:

“Authority”	means the party acting under this Data Protection Protocol as the Controller, and as identified within the signature block.
“Contract”	means the contract entered into by the Commissioners and the Supplier for the delivery of the System;
“Controller”	means the Data Controller and the Party that shares Personal Data under its control, as set out in the UK GDPR;
“Data Loss Event”	means any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Protocol, and/or actual or potential loss and/or destruction of Personal Data in breach of this Protocol, including any Personal Data Breach;
“Data Protection Impact Assessment”	means an assessment of the impact of the envisaged Processing on the protection of Personal Data;
“Data Protection Legislation”	means the Data Protection Act 2018 and the UK GDPR and any other applicable laws of England and Wales relating to the protection of Personal Data and the privacy of individuals (all as amended, updated, replaced, or re-enacted from time to time);
“Data Protection Officer” and “Data Subject”	shall have the same meanings as set out in the UK GDPR;
“Data Subject Access Request”	means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.
“Personal Data”	shall have the same meaning as set out in the UK GDPR;
“Personal Data Breach”	shall have the same meaning as set out in the UK GDPR;
“Processing”	shall have the same meaning as set out in the UK GDPR;
“Processor”	shall have the same meaning as set out in the UK GDPR;

“Protective Measures”	means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data are restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it;
“Protocol” or “Data Protection Protocol”	means this Data Protection Protocol;
“Sub-processor”	means any third party appointed to Process Personal Data on behalf of the Supplier related to this Protocol.
“Supplier”	means Monmedical Limited., trading as Cinapsis.
“System”	means the software, associated documentation and services deployed by the Supplier in support of the Service.
“UK GDPR”	has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018; and
“Users”	means persons authorised by the Authority, Authorised Users, to use the System, and who are bound by this protocol.

1 DATA PROTECTION

- 1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Supplier is the Processor. The only Processing that the Supplier is authorised to do is listed in Table A of this Protocol by the Authority and may not be determined by the Supplier.
- 1.2 The Supplier shall notify the Authority immediately if it considers that any of the Authority's instructions infringe the Data Protection Legislation.
- 1.3 The Supplier shall provide all reasonable assistance to the Authority in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Authority, include:
 - 1.3.1 a systematic description of the envisaged Processing operations and the purpose of the Processing;
 - 1.3.2 an assessment of the necessity and proportionality of the Processing operations in relation to the Services;
 - 1.3.3 an assessment of the risks to the rights and freedoms of Data Subjects; and
 - 1.3.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
- 1.4 The Supplier shall, in relation to any Personal Data processed in connection with its obligations under this Protocol:
 - 1.4.1 process that Personal Data only in accordance with Table A of this Protocol, unless the Supplier is required to do otherwise by Law. If it is so required the Supplier shall promptly notify the Authority before Processing the Personal Data unless prohibited by Law;
 - 1.4.2 ensure that it has in place Protective Measures, which have been reviewed and approved by the Authority as appropriate to protect against a Data Loss Event having taken account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Data Loss Event;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
 - 1.4.3 ensure that :
 - (i) the Supplier Personnel do not Process Personal Data except in accordance with this Protocol (and in particular Table A of this Protocol);
 - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data and ensure that they:
 - (A) are aware of and comply with the Supplier's duties under this Protocol;
 - (B) are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor;

- (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Authority or as otherwise permitted by this Protocol; and
- (D) have undergone adequate training in the use, care, protection and handling of Personal Data;

1.4.4 not transfer Personal Data outside of the EU unless the prior written consent of the Authority has been obtained and the following conditions are fulfilled:

- (i) the Authority or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the GDPR or Article 37 of the Law Enforcement Directive (Directive (EU) 2016/680)) as determined by the Authority;
- (ii) the Data Subject has enforceable rights and effective legal remedies;
- (iii) the Supplier complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Authority in meeting its obligations); and
- (iv) the Supplier complies with any reasonable instructions notified to it in advance by the Authority with respect to the Processing of the Personal Data;

1.4.5 at the written direction of the Authority, delete or return Personal Data (and any copies of it) to the Authority, unless the Supplier is required by Law to retain the Personal Data.

1.5 Subject to Clause 1.6 of this Protocol, the Supplier shall notify the Authority immediately if it:

1.5.1 receives a Data Subject Access Request (or purported Data Subject Access Request);

1.5.2 receives a request to rectify, block or erase any Personal Data;

1.5.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

1.5.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under this Protocol;

1.5.5 receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

1.5.6 becomes aware of a Data Loss Event.

1.6 The Supplier's obligation to notify under Clause 1.5 of this Protocol shall include the provision of further information to the Authority in phases, as details become available.

1.7 Taking into account the nature of the Processing, the Supplier shall provide the Authority with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause 1.5 of this Protocol (and insofar as possible within the timescales reasonably required by the Authority) including by promptly providing:

1.7.1 the Authority with full details and copies of the complaint, communication or request;

- 1.7.2 such assistance as is reasonably requested by the Authority to enable the Authority to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
 - 1.7.3 the Authority, at its request, with any Personal Data it holds in relation to a Data Subject;
 - 1.7.4 assistance as requested by the Authority following any Data Loss Event;
 - 1.7.5 assistance as requested by the Authority with respect to any request from the Information Commissioner's Office, or any consultation by the Authority with the Information Commissioner's Office.
- 1.8 The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this Protocol.
- 1.9 The Supplier shall allow for audits of its Processing activity by the Authority or the Authority's designated auditor.
- 1.10 The Supplier shall designate a Data Protection Officer.
- 1.11 Before allowing any Sub-processor to process any Personal Data related to this Protocol, the Supplier must:
- 1.11.1 notify the Authority in writing of the intended Sub-processor and Processing;
 - 1.11.2 obtain the written consent of the Authority;
 - 1.11.3 enter into a written agreement with the Sub-processor which give effect to the terms set out in this Protocol such that they apply to the Sub-processor; and
 - 1.11.4 provide the Authority with such information regarding the Sub-processor as the Authority may reasonably require.
- 1.12 The Supplier shall remain fully liable for all acts or omissions of any Sub-processor.
- 1.13 The Authority may, at any time on not less than 30 Business Days' notice, revise this Protocol by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Protocol).
- 1.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Authority may on not less than 30 Business Days' notice to the Supplier amend this Protocol to ensure that it complies with any guidance issued by the Information Commissioner's Office.
- 1.15 The Supplier shall comply with any further instructions with respect to Processing issued by the Authority by written notice. Any such further written instructions shall be deemed to be incorporated into Table A from the date at which such notice is received by the Supplier.
- 1.16 Subject to Clauses 1.13, 1.14, and 1.15 of this Protocol, any change or other variation to this Protocol shall only be binding once it has been agreed in writing and signed by an authorised representative of both Parties.

AGREEMENT SIGNATURES

Signed for and on behalf of the Authority:	
Organisation Name:	
Organisation Address:	
Signature:	
Name:	
Position in organisation:	[Caldicott Guardian/SIRO/senior executive or equivalent]
Date:	[dd/mm/yyyy]


Signed for and on behalf of the Supplier:	
Organisation Name:	Monmedical Limited (Trading as Cinapsis)
Organisation Address:	Profile West Suite 2, First Floor, 950 Great West Road, Brentford, United Kingdom, TW8 9ES
Signature:	
Name:	Owain Rhys Hughes
Position in organisation:	CEO
Date:	6 June 2023

Table A – Processing, Personal Data and Data Subjects

Description	Details
Subject matter of the Processing	<p><i>This Agreement relates to the instructions given to the Supplier by the Authority in relation to use of the System.</i></p> <p><i>The Authority is the Controller; the Supplier is the Processor.</i></p> <p><i>Processing relates to the deployment of the System, and it being used to support communications made between clinicians, other healthcare staff and patients, about their ongoing care and referrals to other care settings.</i></p> <p><i>The provision of direct patient care requires the sharing of both personal and special category data among clinicians and other healthcare staff using the System.</i></p>
Duration of the Processing	<p><i>This agreement will run for the duration of the contract made between the Supplier and the Commissioners.</i></p>
Nature and purposes of the processing	<p><i>The System is being deployed by the Commissioner(s) to facilitate the required secure communications routines between clinicians and other healthcare staff that are engaged in the Service.</i></p> <p><i>Under data protection legislation, the Supplier is acting as the Processor operating, at all times, under instructions from the respective data-controller, healthcare providers.</i></p> <p><i>The System enables clinicians to communicate and share information to support clinical decision making for patient care.</i></p> <p><i>Communications between clinicians, other healthcare staff and patients are facilitated through integration with NHS Digital and other electronic patient record systems, use of the encrypted email systems deployed across the NHS, and connectivity to Health and Social Care Network (HSCN) services, as well as encrypted communications over the internet.</i></p> <p><i>Clinicians and other healthcare staff wishing to seek advice or communicate about patient care, will initiate the communication process by input of the patient NHS number, or patient demographic information into the</i></p>

software or directly from the electronic patient record. In turn, the system queries the NHS Spine Service or the electronic patient record system and returns the full patient demographic details, where available. A presenting complaint and, if necessary, additional information such as documents or images are added, which creates a 'Case' within the System. The clinician can then seek advice and/or communicate with a colleague electronically either synchronously, over the telephone or video, or asynchronously through messaging.

Where required, clinicians and other healthcare staff may communicate with patients to request updated or additional information by video, messaging or telephone. Information and images may be supplied to clinicians by patients directly, using a secure web link, or through a video consultation through the System.

The outcomes of patient referrals, including all communications undertaken via voice, video, or written text, are recorded, documented, and stored within the System. Once concluded, Post Episode Messages (PEMs) are distributed for notification and patient administration purposes to the clinical teams involved and their administrative teams, where required.

The System supports Role Based Access - access to clinical components and personal data is restricted to clinicians, and unless requested by the data controller concerned, administrators are only able to access non-clinical and transactional data.

All data processed via the System are encrypted during transmission and whilst at rest on computer servers, located at NHS HSCN accredited data hosting centres, operated by Amazon Web Services EMEA SARL (AWS) and Hicom Technology Limited in the UK. The System is maintained at the data hosting centres by Cinapsis and Hicom Technology Limited.

All voice, voice-to-text, and video files are created in real time, employing encryption, via specialist cloud-based applications. As and when the communication between the participating clinicians ends, an encrypted record is saved within the Cinapsis application, for record storage purposes.

Two suppliers provide the specialist applications, managing the voice, voice-to-text, and video communications, namely, Twilio Ireland Ltd., and Amazon Web Services

	<p><i>EMEA SARL, Ireland (AWS).</i></p> <p><i>The Supplier has in place contracts with Hicom Technology, AWS and Twilio Ireland Ltd., that reflect obligations on confidentiality under this protocol and data protection legislation. These nominated suppliers are regarded as sub-processors of personal data.</i></p> <p><i>The system supports routine access to data by nominated clinicians and healthcare team members, only. All access is managed via secure log-in credentials, which are assigned through security controls.</i></p> <p><i>Ad-hoc requests by Users for support in addressing technical issues arising will be raised with Cinapsis via the help-desk function. Each request will act as an instruction by the User to Cinapsis to administer the system on the User's behalf.</i></p> <p><i>The nature and purpose of the processing has been subjected to a data protection impact assessment in accordance with Data Protection Legislation.</i></p>
<p>Type of Personal Data</p>	<ul style="list-style-type: none"> • Name • Address • Date of birth • NHS Number • MRN, hospital number • Contact details • Full medical records (patient diagnoses, comorbidities, surgical treatments, and interventions)
<p>Categories of Data Subject</p>	<p><i>Patients, clinicians, and associated healthcare professionals and staff.</i></p>
<p>Plan for return and destruction of the data once the Processing is complete UNLESS requirement under union or member state law to preserve that type of data</p>	<p><i>All Personal Data Processed by the Supplier on behalf of the Authority shall be returned by the Supplier to the Authority or destroyed by the Supplier, under instruction from the Authority, and in accordance with the termination and exit agreements made between the parties.</i></p>