

## ECONSULT AND ECONSULT SMART INBOX DATA PROCESSING AGREEMENT

This is an agreement (“Data Processing Agreement”) between the following parties:

1. the healthcare and/or social care organisation that uses eConsult's Services to process data pertaining to patients (the "Healthcare Organisation"); and
2. eConsult Health Ltd, whose registered office is at 85 Great Portland Street, London, England, W1W 7LTJ (Company registration number 07628675)

Recitals

3. eConsult has developed a software application that consists of a range of products to support healthcare organisations. eConsult is used to communicate with and between patients, healthcare and/or social care professionals involved in the patient's care.
4. The Healthcare Organisation is the Controller of and appoints eConsult as its Processor to process Personal Data in order to provide the Services.
5. This Data Processing Agreement regulates the provision and use of Personal Data and ensures both eConsult and the Healthcare Organisation meet their obligations under the Data Protection Legislation.

### 1. Definitions and Interpretations

1.1 The following words and phrases used in this Data Processing Agreement shall have the following meanings, except where otherwise stated or the context otherwise requires:

**eConsult's Sub-Processor List:** Current Sub-Processors are listed in this agreement.

**eConsult's Security Measures Document:** available on request

**Controller** means a natural or legal person or organisation who determines the purposes for which, and the manner in which, any Personal Data are, or are to be processed.

**Processor** in relation to Personal Data, means any person (other than an employee of the Controller) who processes Personal Data on behalf of the Controller.

**Data Protection Legislation** means the EU's General Data Protection Regulation (2016/679), the Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003, the UK GDPR and any mandatory guidance or codes of practice issued by the UK's Information Commissioner's Office from time to time.

**Data Subject** means an individual to whom Personal Data relates.

**GP Medical Record** means the patient's medical record held by their registered GP. GP medical records include, but are not limited to, information about a patient's medicine, allergies, vaccinations, previous illnesses and test results, hospital discharge summaries, appointment letters and referral letters.

**Personal Data** means any information related to an identifiable natural person which can identify that individual, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Special Categories of Personal Data** means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

**Services** means the provision of certain Software by eConsult to the Healthcare Organisation from time to time, including products currently offered and those offered in the future.

**Software** means the software service provided by eConsult Ltd; this software consists of a range of products to support workflow and communication with and between healthcare organisations, healthcare professionals and their patients.

**UK GDPR** has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the UK's Data Protection Act 2018

## 2. Scope of this Data Processing Agreement

2.1 This Data Processing Agreement applies to all data processing activities undertaken by eConsult on behalf of the Healthcare Organisation, except those specific data processing activities within the scope of another agreement that both eConsult and the Healthcare Organisation are party to.

2.2 This Data Processing Agreement constitutes the written instructions of the Healthcare Organisation to eConsult to process Personal Data in the manner described in the Schedule. Such instructions may be supplemented by the Healthcare Organisation from time to time if, for example, the Healthcare Organisation elects to use a new Service offering provided by eConsult or decides to no longer use a particular element of the Services.

### 3. Duration and termination

- 3.1 This Data Processing Agreement shall remain in full force and effect for as long as the Healthcare Organisation continues to use the Services.
- 3.2 Once the Healthcare Organisation no longer uses the Services no new Personal Data shall be collected by eConsult and any Processing shall be subject to the terms hereof as set out in the Schedule

### 4. Governing law and jurisdiction

- 4.4 This Data Processing Agreement is governed by and construed in accordance with the laws of England and Wales.
- 4.5 Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this Data Processing Agreement, or its subject matter or formation.

### 5. Obligations of the Data Controller

- 5.1 The Healthcare Organisation and eConsult acknowledge that, for the purpose of the Data Protection Legislation;
  - 5.1.1 the Healthcare Organisation is the Controller and eConsult is the Processor;
  - 5.1.2 the Healthcare Organisation retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including but not limited to providing any required notices and obtaining any required consents, and for the processing instructions it gives to eConsult.
- 5.2 The Healthcare Organisation warrants and represents that eConsult's processing of Personal Data as contemplated under this Data Processing Agreement will comply with the Data Protection Legislation.
- 5.3 The Healthcare Organisation acknowledges that:
  - 5.3.1 it is responsible for ensuring its use of eConsult to communicate with Data Subjects is appropriate and complies with Data Protection Legislation; and
  - 5.3.2 it must not use the Services in a manner which is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive.

5.4 The Schedule to this Agreement has been reviewed and approved by the Healthcare Organisation and sets out:

- 5.4.1 the types of Personal Data and categories of Data Subject whose Personal Data are Processed;
- 5.4.2 the categories of Processing carried out under this Data Processing Agreement; and
- 5.4.3 a description of the technical and organisational measures adopted by eConsult to protect the Personal Data.

5.5 eConsult shall create and maintain a register which includes the details set out in the Schedule, as well as each transfer of Personal Data to a territory outside of the UK and, where relevant, the documentation of suitable safeguards.

## 6. **Obligations of eConsult**

### 6.1 Processing Instructions

- 6.1.1 eConsult will not process the Personal Data in any other way or in a way that does not comply with this Data Processing Agreement or the Data Protection Legislation. eConsult will notify the Healthcare Organisation immediately if, in eConsult's opinion, the Healthcare Organisation's instructions infringe Data Protection Legislation.
- 6.1.2 eConsult shall comply with any Healthcare Organisation instruction to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.
- 6.1.3 eConsult shall maintain the confidentiality of the Personal Data and not disclose the Personal Data to third parties, unless the Healthcare Organisation or this Data Processing Agreement specifically authorises the disclosure, or as required by domestic law, court or regulator (including the Information Commissioner's Office). If a domestic law, court or regulator requires eConsult to process or disclose the Personal Data to a third party, eConsult must first inform the Healthcare Organisation of such legal or regulatory requirement and give the Healthcare Organisation an opportunity to object or challenge the requirement, unless the domestic law prohibits the giving of such notice.

6.1.4 eConsult shall delete or return all Personal Data to the Healthcare Organisation, at the choice of the Healthcare Organisation, once processing has ceased according to this Data Processing Agreement and shall provide confirmation that all copies of the Personal Data have been deleted within 90 days of such request. eConsult shall retain two pseudonymised data fields, listed in the Schedule, for audit and development purposes.

## 6.2 Rights of the Data Subject

6.2.1 eConsult shall, at no additional cost to the Healthcare Organisation, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Healthcare Organisation as the Healthcare Organisation may reasonably require, to enable the Healthcare Organisation to comply with:

6.2.1.1 the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify, port and erase Personal Data, object to the processing and automated processing of Personal Data, and restrict the processing of Personal Data; and

6.2.1.2 information or assessment notices served on the Healthcare Organisation by the Information Commissioner's Office under the Data Protection Legislation.

6.2.2 eConsult shall notify the Healthcare Organisation promptly in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

6.2.3 eConsult shall notify the Healthcare Organisation within 5 working days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation. Subject to clause 6.17, if eConsult receives a request or other correspondence from a Data Subject, and such communication relates to the Personal Data eConsult is processing on behalf of the Healthcare Organisation, eConsult shall be entitled to respond to the Data Subject directly, but only to the extent necessary to assist the Data Subject in raising their response directly with the Healthcare Organisation. The provisions of this clause requiring eConsult to notify the Healthcare Organisation do not apply in circumstances where eConsult is unable to identify which Healthcare Organisation the relevant Data Subject is linked to (such as where the only information eConsult has about that Data Subject following a communication from them is an email address or mobile phone number).

- 6.2.4 eConsult will give the Healthcare Organisation its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.
- 6.2.5 eConsult shall not disclose the Personal Data to any Data Subject or to a third party other than in accordance with the Healthcare Organisation's written instructions, or as permitted by this Data Processing Agreement, or as required by domestic law.

## 7. Security Measures

- 7.1 eConsult shall at all times implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, copying, modification, reproduction, display, or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure, or damage of Personal Data including, but not limited to, the security measures set out in the Schedule.
- 7.2 eConsult implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:
  - 7.2.1 the pseudonymisation and encryption of Personal Data;
  - 7.2.2 the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
  - 7.2.3 the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
  - 7.2.4 a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

## 8. Compliance

- 8.1 eConsult will reasonably assist the Healthcare Organisation with meeting the Healthcare Organisation's compliance obligations under the Data Protection Legislation, taking into account the nature of eConsult's processing and the information available to eConsult, including in relation to Data Subjects' rights. eConsult shall appoint an individual within eConsult to act as a point of contact for any enquiries from the Healthcare Organisation relating to the Personal Data eConsult is processing on behalf of the Healthcare Organisation. They can be contacted at [dpo@econsult.health](mailto:dpo@econsult.health).

## 9. Audit

9.1 The Healthcare Organisation and its third-party representatives may audit eConsult's compliance with its Data Processing Agreement obligations, by providing at least 30 days' notice. eConsult will give the Healthcare Organisation and its third-party representatives all necessary assistance to conduct such audits.

9.2 The notice requirements in clause 6.13 will not apply if the Healthcare Organisation reasonably believes that a Personal Data breach occurred or is occurring, or eConsult is in breach of any of its obligations under this Data Processing Agreement or any Data Protection Legislation.

## 10. Security breaches

10.1 eConsult shall within 48 hours and in any event without undue delay notify the Healthcare Organisation if it becomes aware of:

10.1.1 the loss, unintended destruction or damage, corruption, or un-usability of part or all of the Personal Data. eConsult will use its reasonable endeavours to restore such Personal Data at its own expense as soon as possible;

10.1.2 any accidental, unauthorised, or unlawful processing of the Personal Data; or

10.1.3 any Personal Data breach.

10.2 Immediately following any accidental, unauthorised or unlawful Personal Data processing or Personal Data breach, the parties will co-ordinate with each other to investigate the matter. Further, eConsult will reasonably co-operate with the Healthcare Organisation in the Healthcare Organisation's handling of the matter

10.3 eConsult will not inform any third party of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data breach without first obtaining the Healthcare Organisation's written consent, except when required to do so by domestic law.

10.4 eConsult agrees that the Healthcare Organisation has the sole right to determine:

10.4.1 whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data breach to any Data Subjects, the Information Commissioner's Office, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Healthcare Organisation's discretion, including the contents and delivery method of the notice. Save that nothing in this clause shall prevent eConsult from making any notifications required to maintain any insurance cover, regulatory authorisations, or avoid being in contractual breach of any other agreement it has entered into; and

10.4.2 whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

## 11. eConsult personnel

11.1 eConsult must ensure that eConsult personnel processing the data on eConsult's behalf are subject to a duty of confidentiality ensuring in each case that access is strictly limited to those employees who need to access the relevant Personal Data, as strictly necessary to perform the Services in the context of that employee's duties to eConsult, ensuring that all such employees:

- 11.1.1 are aware of and comply with eConsult's duties under this Data Processing Agreement;
- 11.1.2 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 Healthcare Organisation or as otherwise permitted by this Data Processing Agreement;
- 11.1.3 are subject to user authentication and log on processes when accessing the Personal Data; and
- 11.1.4 have undertaken appropriate training in relation to Data Protection Legislation and in the use, care, protection and handling of the Personal Data.

11.2 eConsult shall maintain up-to-date compliance with the NHS Data Security and Protection Toolkit (DSPT).

## 12. Sub-Processors

12.1 The Healthcare Organisation gives eConsult a general written authorisation for the engagement of third-party sub-processors for the processing of Personal Data, subject to the terms of this Data Processing Agreement, Art. 32 of the UK GDPR, and the rules on transfers to third countries. The sub-processors currently used by eConsult are set out on eConsult's Sub-Processor List.

12.2 eConsult shall carry out due diligence on each sub-processor to ensure that it is capable of providing the level of protection for the Personal Data as is required by this Data Processing Agreement. eConsult will include terms in the contract between eConsult and the sub-processor substantially similar to those set out in this Data Processing Agreement, and which are at a minimum compliant with the requirements of the Data Protection Legislation. Upon request, eConsult shall provide a copy of its agreements with sub-processors to the Healthcare



Organisation (which may be redacted to remove confidential information not relevant to the requirements of this Data Processing Agreement).

- 12.3 eConsult will notify the Healthcare Organisation of any intended change concerning the addition or replacement of sub processors by updating eConsult's Sub-Processor List. The Healthcare Organisation acknowledges that it is their responsibility to check regularly for any updates to eConsult's Sub-Processors.
- 12.4 The Healthcare Organisation approves the engagement of the entities listed at eConsult's Sub-Processor Webpage as sub-processors of eConsult for the processing of Personal Data. eConsult shall update the list of sub-processors at eConsult's Service Webpage at least 5 days in advance of when a new sub-processor for the processing of Personal Data is engaged.
- 12.5 Where the sub-processor fails to fulfil its obligations under the written agreement with eConsult which contains terms substantially the same as those set out in this Data Processing Agreement, eConsult remains fully liable to the Healthcare Organisation for the sub-processor's performance of its agreement obligations.

### 13. Cross-border Transfers

13.1 The Healthcare Organisation consents to eConsult processing Personal Data outside the UK provided that:

- 13.1.1 eConsult is processing the Personal Data in a territory which is subject to adequacy regulations under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals. eConsult must identify on eConsult's Sub-Processor Webpage the territory that is subject to such adequacy regulations; or
- 13.1.2 eConsult participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that eConsult (and, where appropriate, the Healthcare Organisation) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the UK GDPR. eConsult must identify on eConsult's Sub-Processor Webpage the transfer mechanism that enables the parties to comply with these cross-border data transfer provisions and eConsult must promptly inform the Healthcare Organisation of any change to that status; or
- 13.1.3 the transfer otherwise complies with the Data Protection Legislation.

## 14. **Liability**

14.1 Nothing in this Data Processing Agreement limits any liability which cannot legally be limited, including but not limited to liability for:

14.1.1 death or personal injury caused by negligence; and

14.1.2 fraud or fraudulent misrepresentation.

14.2 Subject to clause 8.1, eConsult's total liability to the Healthcare Organisation under this Data Processing Agreement shall not exceed £1,000,000 (one million pounds)

## 15. Schedule

### Processing, Personal Data and Data Subjects

Description	Details
<b>Subject matter of the processing</b>	<p>To provide the Services (eConsult's service and, if applicable, the additional "Smart Inbox" platform), as adopted by the Healthcare Organisation from time to time.</p>
<b>Duration of the processing</b>	<p>For eConsult (without Smart Inbox) patient data will be retained for up to five weeks. Audit data (pseudonymised and anonymised) will be retained in line with Records Management Code of Practice for Health and Social Care 2016 subject to earlier deletion where Article 9 (3) GDPR and S11.1 Data Protection Act 2018 no longer applies.</p> <p>For eConsult (with Smart Inbox) both patient data and audit data (pseudonymised and anonymised) will be retained in line with Records Management Code of Practice for Health and Social Care 2016 subject to earlier deletion where Article 9 (3) GDPR and S11.1 Data Protection Act 2018 no longer applies.</p>
<b>Purposes and nature of the processing</b>	<p>The purposes and nature of the processing includes:</p> <ul style="list-style-type: none"> <li>• Communication between patients, healthcare and/or social care professionals, via SMS, email, forms, NHS App, or other electronic communication, which may include images or documents.</li> <li>• Triage workflow of incoming consultations, including management of responses to these incoming consultations.</li> <li>• Video and audio communication for the purposes of video / phone consultation.</li> <li>• Appointment booking and recording solution.</li> <li>• Record view for viewing GP Medical Records</li> <li>• For users of Smart Inbox - saving and coding activity from the Smart Inbox into the clinical system(s). This includes searching for the patient records in the clinical system to match to the correct record, and optimisation of that search to speed up processing (e.g. caching).</li> <li>• Healthcare and/or social care professionals may disclose patient data to eConsult when receiving technical support and from time-to-time eConsult's technical team may have access to patient data when they are fixing a technical issue for</li> </ul>

	<p>example via remote support, which may include screen sharing.</p> <ul style="list-style-type: none"> <li>• Compilation of anonymised statistics about the use of eConsult's platform, such as the use of its functions by its users in communication with patients. These statistics may be used for eConsult's own analytics and improvement purposes. eConsult may also share these anonymised statistics publicly or with third parties. These third parties include: <ul style="list-style-type: none"> <li>• national bodies, including NHS Digital and NHS England;</li> <li>• local NHS bodies, including CCGs and Primary Care Networks;</li> <li>• partners of eConsult, including commercial organisations, charities and academic institutions.</li> </ul> </li> </ul>
Description	Details
<p><b>Type of Personal Data</b></p>	<p>Personal Data (relating to patients of the Data Controller):</p> <ul style="list-style-type: none"> <li>• Patient demographic details (name; date of birth; gender)</li> <li>• NHS number</li> <li>• Mobile phone number</li> <li>• Email address</li> </ul> <p>Personal Data (relating to healthcare and/or social care professionals):</p> <ul style="list-style-type: none"> <li>• Name</li> <li>• Email address</li> <li>• Mobile phone number</li> <li>• Affiliated organisations</li> <li>• Job role</li> </ul> <p>Sensitive Personal Data:</p> <ul style="list-style-type: none"> <li>• Content of the communications with – or regarding - patients sent via the Services (which may include patient images or documents and contain data concerning health).</li> <li>• Other types of data, including third party data, (which may include contents of the patient's GP Medical Record and data concerning health that may from time to time be required to provide the Services). This includes two pseudonymised data fields (date of birth of patient and gender) that are retained by eConsult for audit and development purposes for a period of up to eight years then review.</li> </ul>

<b>Security Measures adopted by eConsult</b>	As set out eConsult's Data Security Document.
<b>Approved Sub-Processors</b>	<p>As set out on eConsult's Sub-Processor List. As of January 2024, the list comprises:</p> <p><b>Amazon Web Services:</b> (main hosting provider) all data held in UK instances.</p> <p><b>Atlas - Amazon Web Services:</b> all data held in UK instances.</p> <p><b>Redcentric PLC</b> - used for secure transmission of data from AWS UK to end users when routing via HSCN is required.</p> <p><b>Auth0:</b> used for authentication services.</p> <p><b>Hero Health:</b> used for integration with appointment booking and messaging.</p> <p><b>CookieFirst:</b> used for providing a standardised, compliant approach to cookie management. No patient data involved.</p> <p><b>Codacy:</b> used to check code accuracy and security, data transferred outside the UK based on adequacy and standard contractual clauses, no patient data involved.</p> <p><b>Datadog:</b> used to check security and performance monitoring. EU data centres, no patient data involved.</p> <p>Delighted: used for non-mandatory feedback, data transferred outside the UK based on adequacy and standard contractual clauses.</p> <p><b>Firetext:</b> text messaging, all data held in the UK.</p> <p>Hotjar: user analytics and feedback - User and usage data that Hotjar collects through its software is stored in Ireland, European Union (EU) on the Amazon Web Services infrastructure, eu-west-1 data centres.</p> <p><b>Mixpanel:</b> used for analytics. No patient data. For customers participating in the EU residency program, data is stored in the Google Cloud Platform's Europe-West 4 data centre (Eemshaven, Netherlands).</p> <p><b>Pusher.com:</b> used to allow communication between instances of the application. No patient data. Data is processed in the European Economic Area (EEA)</p>