NHS England

Data Processing Agreement for Sample

NHS England
Dental Referral Management Service (DRMS)

January 2018

Version No. 2

Table of Contents

1 Parties to the Agreement

1.1 Parties

This Data Processing Agreement (Agreement) is drawn up between…	
Organisation Name:	**{$ORGANISATION}**
Organisation Address:	{$ADDRESS1} {$ADDRESS2} {$ADDRESS3} {$ADDRESS4} {$POSTCODE}
…hereinafter known as the Data Controller and…	
Organisation Name:	**FDS Consultants**
Organisation Address:	Referral Management Centre Stannian Fold, Lymm Warrington, Cheshire, WA16 6LU
…hereinafter known as the Data Processor.	

1.2 Scope of Agreement

Start Date	**{$START}**	End Date	**31st March 2022**

2 Agreement Terms

2.1 Introduction

2.1.1 FDS Consultants (the Data Processor) is required by its contract agreement with NHS England to issue this Data Processing Agreement at this point. Any queries linked to this agreement should be raised with NHS England. In terms of FDS compliance with the General Data Protection Regulation (GDPR) (and any legislation introduced by the UK) we will comply with *all aspects of the legislation* as required. This includes redefined responsibilities for data controllers and data processors. It should also be noted that FDS maintains and completes an IG Toolkit Return has commenced activities linked to the new Data Security and Protection Toolkit. FDS has also appointed a service to provide its Data Protection Officer function in recognition of the types of data that it is required to process. Further information on our approach to GDPR can be found on our website at https://www.dental-referrals.org/gdpr/ and you can view our IGTK submission using our organisation code 8J025.

2.1.2 This Agreement provides an operating framework to enable lawful disclosure of NHS information to and data processing by the Data Processor working on behalf of the Data Controller taking account of the Data Protection Act 1998, and NHS guidance on confidentiality of personal information, the common law duty of confidence and other applicable legislation.

2.1.3 The terms and conditions of this Agreement shall apply to all Information provided by the Data Controller, or obtained by the Data Processor from other sources as part of the delivery of the contracted services, or derived from any combination thereof.

2.1.4 This Agreement between the Data Controller and the Data Processor supports all data processing in relation to contracts between the Processor and NHS England related to the management of dental referrals.

2.2 Definitions

2.2.1 **Personal data*** any factual information or expressions of opinion relating to an individual who can be identified directly from that information or in conjunction with any other information that is held by or comes into the possession of the data holder.

2.2.2 **Sensitive personal data*** the eight categories of personal information defined as sensitive personal data in section 2 of the Data Protection Act 1998 (DPA) and, in this Agreement specifically including (but not limited to) information about the physical & mental health, racial or ethnic origin, sexual life or sexuality of patients or service users.

2.2.3 **Confidential Information*** any information or combination of information that contains details about an organisation or an individual person that was provided in an expectation of confidence. This includes for example, non-personal corporate or technical information that is commercially sensitive,

drafts of documents that are not ready for publication, restricted information & documents, etc. as well as personal data about patients, service users and staff.

2.2.4 **Information*** any information as defined in *Section 2.2.1* to *Section 2 2.3* that the Data Controller owns. This includes all information supplied to the Data Processor by the Data Controller and any additional information that the Data Processor obtains during the term of the contract and shall apply equally to original Information and all back-up and/or copies printed out.

2.2.5 **Data Controller*** as defined in the Data Protection Act (1998) is the individual or organisation (legal person) who determines the manner and purpose of the processing personal information, including what information will be processed and how it will be obtained.

2.2.6 **Data Processor*** as defined in the Data Protection Act 1998, is an individual (other than an employee of the data controller) or organisation who processes personal information whilst undertaking a business activity or service on behalf of the Data Controller, under contract.

2.2.7 **Data Processing*** also defined in the Data Protection Act 1998 in respect of personal data, for the purpose of this document this includes any business activity or contracted service that involves using personal, corporate or other information including obtaining, recording, holding, viewing, storing, adapting, altering, deleting, disclosing. This is not restricted to computer processing, but includes manual files and verbal discussions.

2.3 General Terms

2.3.1 The Data Processor shall put in place appropriate technical and organisational measures to ensure the protection of the Information subject to this Agreement against the accidental loss or destruction of or damage to Information, having regard to the specific requirements set out in this Agreement, the state of technical development and the level of harm that may be suffered the Data Controller and/or by a Data Subject whose Personal data is affected, by such unauthorised or unlawful processing or by its loss, damage or destruction.

2.3.2 All Information referred to in *Section 2.2.4* above remains the property of the Data Controller and shall be either returned or destroyed by the Data Processor after a period of one year after completion of the contracted service, in a manner previously agreed with the Data Controller

2.3.3 Under the terms of this Agreement the Data Controller shall provide the Data Processor with the minimum amount of Information necessary to deliver the contracted service and, in particular, personal and sensitive information will be supplied on a restricted ‘need to know’ basis.

2.3.4 The Data Processor shall only process information as is necessary to perform its obligations under this Agreement and only in accordance with any instruction given by the Data Controller under this Agreement and, in particular shall not use or process Information for any purpose other than as directed by the Data Controller for delivery of the contracted service.

2.3.5 The Data Processor shall not subcontract any of its processing operations performed on behalf of the data controller under this Agreement without the prior written consent of the Data Controller. Where the Data Processor subcontracts its obligations, with the consent of the Data Controller, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data processor under this Agreement. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data processor shall remain fully liable to the data controller for the performance of the sub-processor's obligations under such agreement.

2.3.6 Any minor changes to this Agreement that may become necessary from time to time shall be made by the Data Controller to the Data Processor, or requested by the Data Processor from the Data Controller, as a written variation.

2.3.7 In the event of major changes being required, the Data Controller shall terminate this Agreement and replace in full with an updated version. Such termination and replacement may also be initiated by the Data Processor, subject to prior arrangement with the Data Controller.

2.4 Description of Information

2.4.1 The information covered in this Agreement is as detailed in *Section 2.4.2* and where relevant is indicated as personal, sensitive or confidential as defined in *Sections 2.2.1, Section 2.2.2* and *Section 2.2.3* respectively. The Data Processor shall not disclose information to any third party without the prior written agreement of the Data Controller. Disclosure of such data as may contain patient information will require evidence of Caldicott Guardian approval before disclosure for the purpose of delivery of the contracted service. Other data which may be considered ‘corporate confidential’ or contains information which is sensitive or otherwise person identifiable will require evidence of SIRO and\or Caldicott Guardian approval (as appropriate) before disclosure for the purpose of delivery of the contracted service. In such cases where the signatory to this agreement, acting on behalf of the Data Controller, is not the Caldicott Guardian or SIRO (as appropriate), copies of such approval should be furnished to the aforementioned signatory before he\she signs this document.

2.4.2 The information covered by this Agreement comprises:

- Data required for the purpose of referring a patient between healthcare services and for managing these referrals.
- Data necessary for communication between healthcare organisations and professionals in relation to patient referrals.
- Data relating to users of the service necessary for the security and management of the service.

2.5 Data Protection

2.5.1 The Data Processor shall comply with all aspects of the Data Protection Act 1998, Human Rights Act 1998 and common law duty of confidentiality in relation to the processing of personal data and sensitive personal data as part of this Agreement

2.5.2 The Data Processor shall only process data in accordance with the instruction of the Data Controller as specified under this Agreement

2.5.3 The Data Processor shall put in place appropriate technical and organisational measures against any unlawful and unauthorised processing of Information and against accidental loss, destruction of and damage to Information.

2.5.4 The Data Processor shall not cause or allow Information to be transferred to any territory outside the European Economic Area without the prior written permission of the Data Controller.

2.6 Policies and Procedures

2.6.1 The Data Processor shall have confidentiality, information security, data protection and records management policies. These will describe individual responsibilities for handling Information and will be rigorously applied.

2.6.2 The Data Processor shall provide the Data Controller with copies of the policies referred to in *Section 2.6.1* above on request or as appendices to this Agreement.

2.7 Data Processor Employees

2.7.1 The Data Processor shall undertake all reasonable background checks to ensure the reliability of all employees who are likely to use or have access to the Information.

2.7.2 The Data Processor shall include appropriate confidentiality clauses in employment contracts, including details of sanctions against any employee acting in a deliberate or reckless manner that breaches confidentiality or the non-disclosure provisions of DPA or causes damage to or loss of Information.

2.7.3 The Data Processor shall ensure that all employees are aware of and act in accordance with the policies referred to in *Section 2.6.1* above.

2.7.4 The Data Processor shall ensure that all employees are adequately trained to understand and comply with their responsibilities under DPA, the common law duty of confidence and this Agreement and shall provide the Data Controller with evidence of that training on request or as appendices to this Agreement.

2.7.5 Subject to *Sections 2.7.1 to 2.7.4*, the Data Processor shall ensure that only those employees involved in delivery of the contracted service use or have access to Information on a strict 'need to know' basis and shall implement appropriate access controls to ensure this requirement is satisfied.

2.7.6 The Data Processor shall ensure that any employees involved in delivery of the contracted service who do not specifically need to use personal information as part of their role have restricted access to anonymised Information and/or redacted extracts only.

2.8 Security – General

2.8.1 The Data Controller will not contract services from Data Processors unable or unwilling to comply with the terms of this Agreement and reserves the right to terminate the contract if either party is unable to agree necessary amendments in future.

2.8.2 The Data Processor shall not under any circumstances share, disclose or otherwise reveal Information (in whole or in part) to any individual, business or other organisation (third party) not directly involved in delivery of the contracted service without the explicit written consent of the Data Controller.

2.8.3 The Data Processor shall notify the Data Controller immediately of any untoward incidents or activities that suggest non-compliance with any of the terms of this Agreement. This includes 'near miss' situations even if no actual damage to or loss -or inappropriate disclosure of Information results.

2.8.4 The Data Processor shall indemnify the Data Controller against and compensate for any loss (financial or otherwise) that the Data Controller sustains due to any failure by the Data Processor or employees or sub-contractors to act in accordance with the terms of this Agreement and relevant legislation.

2.9 Security – Physical

2.9.1 The Data Processor shall ensure that all information is physically protected from accidental or deliberate loss or destruction arising from environmental hazards such as fire or flood.

2.9.2 The Data Processor shall ensure that all information is held on premises that are adequately protected from unauthorised entry and/or theft of NHS Information or any IT equipment on which it is held by, for example, the use of burglar alarms, security doors, ram-proof pillars, controlled access systems, etc.

2.10 Security – IT Systems

2.10.1 The Data Processor shall hold electronically-based information on secure servers unless otherwise agreed in writing.

2.10.2 Information will, under no circumstances, be stored on portable media or devices such as laptops or USB memory sticks or CD-ROM unless agreed in writing and subject, at a minimum, to those constraints detailed in *Section 2.10.3*.

2.10.3 The Data Processor shall ensure that:

- All portable media used for storage or transit of NHS information are fully encrypted in accordance with NHS Guidelines on encryption to protect personal information (January 2008).
- Portable media are not left unattended at any time (e.g. in parked cars, in unlocked & unoccupied rooms, etc.).
- When not in use, all portable media are stored in a locked area and issued only when required to authorised employees, with a record kept of issue and return.

2.10.4 The Data Processor shall not allow employees to hold Information on their own personal computers.

2.10.5 The Data Processor shall ensure adequate back-up facilities to minimise the risk of loss of or damage to information and that a robust business continuity plan is in place in the event of restriction of service for any reason.

2.10.6 The Data Processor shall not transmit NHS information by email except as an attachment encrypted to 256 bit AES\Blowfish standards or from NHS mail to NHS mail.

2.10.7 The Data Processor shall only make printed paper copies of information if this is essential for delivery of the contracted service.

2.10.8 The Data Processor shall store printed paper copies of information in locked cabinets when not in use and shall not remove from premises unless this is essential for delivery of the contracted service.

2.10.9 The Data Processor shall provide the Data Controller with confirmation that they have a signed Information Governance Statement of Compliance (IGSoC) (as evidence of achieving a minimum of at least a level 2 in respect of the NHS Information Governance Toolkit) OR evidence of compliance with another agreed Information Security Management System (ISMS), before the Data Controller can allow any access to networked IT systems (e.g. N3, Summary Care Record).

2.10.10 Subject to ISMS assurance requirements specified at *Section 2.10.8,* The Data Processor shall complete an annual IG Toolkit assessment.

2.11 Secure Destruction

2.11.1 The Data Processor shall ensure that information held in paper form regardless of whether as originally provided by the Data Controller or printed from the Data Processor's IT systems) is destroyed using a cross cut shredder or subcontracted to a confidential waste company that

complies with European Standard EN15713 (BS15713 (BS 15713) The Secure Destruction of Confidential Material). The Data Processor shall ensure that electronic storage media used to hold or process Information is destroyed or overwritten to current CESG standards as defined at www.cesg.gov.uk

2.11.2 In the event of any bad or unusable sectors that cannot be overwritten, the Data Processor shall ensure complete and irretrievable destruction of the media itself.

2.11.3 The Data Processor shall provide the Data Controller with copies of all relevant overwriting verification reports and/or certificates of secure destruction of NHS information at the conclusion of the contract.

2.12 Monitoring & Audit

2.12.1 The Data Processor shall permit the Data Controller to monitor compliance with the terms of this Agreement, by:

- Allowing Data Controller employees or nominated representatives to enter any premises where information is held, at all reasonable times and with or without prior notice, for the purpose of inspection.
- Completing and returning a Data Processing Monitoring Form at the request of the Data Controller.
- Provide independent assurance of the self-audited Information Governance Toolkit performance measures where the Data Processor is required to comply.

2.13 Freedom of Information

2.13.1 The Data Processor acknowledges that the Data Controller is a public authority for the purpose of the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR).

2.13.2 Basic details of the contract shall be included in the appropriate log under the 'Data Controllers Publication Scheme'.

2.13.3 In addition, the Data Controller may be statutorily required to disclose further information about the contracted service or the contract itself in response to a specific request under FOIA or EIR, in which case:

- The Data Processor shall provide the Data Controller with all reasonable assistance and co-operation to enable the Data Controller to comply with its obligations under FOIA or EIR.
- The Data Controller shall consult the Data Processor regarding commercial or other confidentiality issues in relation to this contract, however the final decision about disclosure of information or application of exemptions shall rest solely with the Data Controller.

2.14 Legal Jurisdiction

2.14.1 This Agreement is governed by and shall be interpreted in accordance with the law of England.

2.14.2 In the event of a dispute, the parties to this Agreement agree to attempt to resolve such issues according to NHS dispute resolution procedures. In the event that agreement cannot be reached, the parties agree that the courts of England shall have exclusive jurisdiction to hear the case.

2.15 Relevant NHS Publications

2.15.1 A range of publications can be obtained from the following websites, including relevant NHS codes of practice and standards:

- https://www.gov.uk/government/organisations/department-of-health
- http://www.nhsemployers.org/Pages/home.aspx
- https://digital.nhs.uk/

These cover areas including confidentiality, information security management, employment check standards and records management. It is the responsibility of the Data Processor to ensure they are compliant with these practices and standards.

3 Data Processing Agreement - Compliance Assurance

To be completed and signed by the Data Processor.

No.	Question	Yes/No/ Not Applicable	Details
1.	If you already process personal data on your own behalf, as defined within the Data Protection Act 1998, have you reviewed your Notification to the Information Commissioner for Data Processing within the past 12 months? If **Yes**, confirm your Notification number.	YES	Registration Number: Z3285272
2.	Do your staff have confidentiality/data protection training at induction and subsequently on an annual basis and are aware of the organisational policies and procedures and are notified when any changes are made?	YES	
3.	Have you had a security breach resulting in loss of or damage to personal or confidential information within the past two years? If **Yes**, include details:	NO	

No.	Question	Yes/No/ Not Applicable	Details
3.	Have you had a security breach resulting in unauthorised disclosure of personal information within the past two years? If **Yes**, include details:	NO	
4.	Have you been the subject of any complaints to the Information Commissioner within the past two years? If **Yes**, include details.	NO	
5.	If you answered **Yes** to any of questions 2 – 4 above, did this affect Information belonging to the Data Controller? If **Yes**, include details.	N/A	
6.	If you answered **Yes** to question 5 above, did the incident result in disciplinary action against any of your employees and /or sub-contractors? If **Yes**, include details.	N/A	
7.	Have you updated or amended your confidentiality, information security, data protection or records management policies since the commencement of the contract? If **Yes**, include details and provide copies if the amendments substantially alter the policy.	NO – See Note	Policies and procedures may change during the GDPR mobilisation period. All information in relation to new policies, training and other GDPR related activities can be found at https://www.dental-referrals.org/gdpr/

No.	Question	Yes/No/ Not Applicable	Details
8.	Are there any other matters that you consider relevant in relation to your compliance with the Data Controller's requirements? If **Yes**, include details.	NO	

I confirm that FDS Consultants is complying with all aspects of the Data Controller's confidentiality and information security requirements as detailed above, described within the NHS IGTK and it successor and within the requirements of the General Data Protection Regulations.	
Signature:	
Name:	ANNE LAMB
Date:	{$START}
Position:	DIRECTOR

4 Agreement Signatures

For and on behalf of the Data Controller	
Signature:	{$imagelinsert_image:150:90}
Name:	{$FIRSTNAME} {$LASTNAME}
Date:	{$START}
Position:	{$POSITION}

For and on behalf of the Data Processor	
Signature:	
Name:	ANNE LAMB
Date:	{$START}
Position:	DIRECTOR

5 Related Documents, Conventions and Glossary

5.1 Related Documents

Title	Reference	Version
The Secure Destruction of Confidential Material	BS EN 15713	

5.2 Typographical Conventions

- Fields, radio buttons etc are shown in **bold**.
- References, including those to external documents, are shown in *italics*.

5.3 Glossary

Term/Acronym	Description
CSU	Commissioning Support Unit
DMIC	Data Management and Integration Centre
DPA	Data Protection Act 1998
DSCRO	Data Service for Commissioners Regional Office
EIR	Environmental Information Regulations 2004
FOIA	Freedom of Information Act 2000
SIRO	Senior Information Risk Owner
GDPR	General Data Protection Regulations