Terms and Conditions of IEP Services

version 12.2

-and-

-and-

Sectra Limited

AGREEMENT
relating to the

Image Exchange Portal Service

Contents

This Agreement is made on the

BETWEEN:

, (“Client”) incorporated and registered in England with company number

whose registered office is at

and

, (“Client”) incorporated and registered in England with company number

whose registered office is at

and

Sectra Limited incorporated and registered in England with company number 4571654 whose registered office is at (“Supplier”).

A. GENERAL PROVISIONS

A1 Definitions and Interpretation

A1.1 In this Contract unless the context otherwise requires the following provisions shall have the meanings given to them below:

“Annual Service Charge” means the annual price exclusive of any setup costs or other onetime costs (exclusive of any applicable VAT), payable to the Supplier by the Client under the Contract, as set out in Schedule Two, but before taking into account the effect of any adjustment of price in accordance with clause C3 (Price Adjustment on Extension of Initial Contract Period).

“Client Staff” means all persons employed by the Client to perform its obligations under the Contract together with the Client’s servants, agents, suppliers and sub-contractors using the Services.

“Commencement Date” means the date at which the service goes live.

“Confidential Information” means any information which has been designated as confidential by either Party in writing or that ought to be

considered as confidential (however it is conveyed or on whatever media it is stored) including information the disclosure of which would, or would be likely to, prejudice the commercial interests of any person, pricing, specifications, trade secrets, Intellectual Property Rights and know-how of either Party and all personal data and sensitive personal data within the meaning of the DPA, provided that Confidential Information shall not include information which:

(i) was public knowledge at the time of disclosure (otherwise than by breach of clause E2 (Confidential Information));

(ii) was in the possession of the receiving Party, without restriction as to its disclosure, before receiving it from the disclosing Party;

(iii) is received from a third party (who lawfully acquired it) without restriction as to its disclosure; or

(iv) is independently developed without access to the Confidential Information.

"Contract" means this written agreement between the Client and the Supplier consisting of these clauses and any attached Schedules.

"Contract Change Notice (CCN)" means a change to this Contract or its associated Schedules which is agreed between both Parties as per B1.2.

"Contract Period" means the period from the Commencement Date to:

(a) the Expiry Date of the Initial Contract Period: or

(b) following an extension pursuant to clause F4 (Extension of Initial Contract Period), the expiry date of the extended period: or

(c) such earlier date of termination of the Contract in accordance with the Law or the provisions of the Contract.

"Contract Price" means the price (exclusive of any applicable VAT) including the Annual Service Charge and any setup costs or other onetime costs, payable to the Supplier by the Client under the Contract, as set out in Schedule Two, but before taking into account the effect of any adjustment of price in accordance with clause C3 (Price Adjustment on Extension of Initial Contract Period).

"Default" means any breach of the obligations of the relevant Party (including but not limited to fundamental breach or breach of a fundamental term) or any other default, act, omission, negligence or negligent statement of the relevant Party or the Client Staff in connection with or in relation to the subject-matter of the Contract and in respect of which such Party is liable to the other.

"Effective Date" means the date of this Agreement

"Expiry Date" means the expiry date detailed in clause F4 (Extension of Initial Contract Period).

"Fault" means a problem with the operation of the Service.

"FOIA" means the Freedom of Information Act 2000 and any subordinate legislation made under this Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant government department in relation to such legislation.

"Force Majeure" means any event or occurrence which is outside the reasonable control of the Party concerned and which is not attributable to any act by that Party, including fire; flood; violent storm; pestilence; explosion; malicious damage; armed conflict; acts of terrorism; nuclear, biological or chemical warfare; or any other disaster, natural or man-made and, in the case of the Supplier, the Service Limitations.

"GDPR" means the UK GDPR as defined in sections 3(10) and 205(4) of the Data Protection Act 2018.

“IEP” means the image exchange portal service; a service allowing the secure transfer of diagnostic images and reports.

“IEP Administrator” means an IEP user at the Client site who has been allocated such role during the initial IEP configuration by the Client or as subsequently assigned to such role by an existing IEP Administrator.

“Information” has the meaning given under section 84 of the FOIA.

“Information Security Standard” means ISO27001:2013

“Initial Contract Period” means the period of 12 months from the Commencement Date

“Intellectual Property Rights” means patents, inventions, trademarks, service marks, logos, design rights (whether registerable or otherwise), applications for any of the foregoing, copyright, database rights, domain names, trade or business names, moral rights and other similar rights or obligations whether registerable or not in any country (including but not limited to the United Kingdom) and the right to sue for passing off.

“Law” means any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, regulatory policy, guidance or industry code, judgment of a relevant court of law, or directives or requirements or any Regulatory Body of which the Supplier is bound to comply.

“Month” means calendar month.

"Operational Helpdesk Hours" means the hours of operation of the Supplier's helpdesk as detailed in the Service Specification Schedule.

"Party" means a party to the Contract.

"Quality Standards" means the quality standard ISO13485:2016.

"Receipt" means the physical or electronic arrival of the invoice at the address of the Client detailed at clause A3.3 or at any other address given by the Client in writing to the Supplier for the submission of invoices.

"Regulatory Bodies" means those government departments and regulatory, statutory and other entities, committees, ombudsmen and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in the Contract or any other affairs of the Client and "Regulatory Body" shall be construed accordingly.

"Request for Information" shall have the meaning set out in FOIA or the Environmental Information Regulations as relevant (where the meaning set out for the term "request" shall apply).

"Schedule" means a schedule attached to, and forming part of, the Contract.

"Services" means the IEP services to be supplied as specified in Schedule One.

"Service Limitations" means all aspects of the transfer process that are outside the direct control of the Supplier, including, but not limited to the performance of the network and performance of equipment at the Client's site or not under the control of the Supplier.

"Service Specification Schedule" means Schedule One of this Contract, containing details of the Services to be supplied under the Contract.

"Staff" means all persons employed or contracted by the Supplier to perform its obligations under the Contract together with the Supplier's servants, agents, suppliers and sub-contractors used in the performance of its obligations under the Contract.

"Staff Vetting Procedures" means the Supplier's procedures for the vetting of personnel.

"Supplier Helpdesk" means support personnel provided by the Supplier to resolve technical or operational issues with the Service.

"Target Resolution Time" means the elapsed time in operational helpdesk hours between the Fault being logged with the Supplier Helpdesk and the Fault being resolved or a workaround being provided by the Supplier Helpdesk.

"the Code" means Secretary of State for Constitutional Affairs Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000

"Training Session" is a maximum of 4 hours for a maximum of four people held on Client premises, Supplier premises or via a remote training session, to be decided at the Supplier's discretion.

"VAT" means value added tax in accordance with the provisions of the Value Added Tax Act 1994.

"Working Day" means a day (other than a Saturday or Sunday) on which banks are open for general business in the City of London.

A1.2 The interpretation and construction of the Contract shall be subject to the following provisions:

(a) words importing the singular meaning include where the context so admits the plural meaning and vice versa;

(b) words importing the masculine include the feminine and the neuter;

(c) reference to a clause is a reference to the whole of that clause unless stated otherwise;

(d) reference to any statute, enactment, order, regulation or other similar instrument shall be construed as a reference to statute, enactment, order regulation, or instrument as amended by any subsequent enactment, modification, order, regulation or instrument as subsequently amended or re-enacted.

(e) reference to any person shall include natural persons and partnerships, firms and other incorporated bodies and all other legal persons of whatever kind and however constituted and their successors and permitted assigns or transferees; and

(f) the words "include", "includes" and "including" are to be construed as if they were immediately followed by the words "without limitation"; and

(g) headings are included in the Contract for ease of reference only and shall not affect the interpretation or construction of the Contract.

A2 Initial Contract Period

The Contract shall be effective from the Effective Date. The service shall start on the Commencement Date and expire 12 months later, unless extended or otherwise terminated in accordance with the provisions of this Contract. There will be an option to extend in increments of 12 months if agreed by both Parties.

A3 Notices

A3.1 Except as otherwise expressly provided within the Contract, no notice or other communication from one Party to the other shall have any validity

under the Contract unless made in writing by or on behalf of the Party concerned.

A3.2 Any notice or other communication which is to be given by either Party to the other shall be given by letter (first class post, recorded delivery or special delivery), or electronic mail with confirmation of receipt. Such letters shall be addressed to the other Party in the manner referred to in clause A3.3.

A3.3 For the purposes of clause A3.2, the address of each Party shall be:

(a) For the Client:

For the attention of:

Email:

Tel:

(b) For the Supplier: Sectra Ltd

For the attention of: Contracts Manager

Email:

A3.4 Either Party may change its address for service by serving a notice in accordance with this clause A3.

B. SUPPLY OF SERVICES

B1 The Services

B1.1 The Supplier shall supply the Services during the Contract Period in accordance with the Schedule One - Service Specification Schedule and the provisions of the Contract in consideration of the payment of the Contract Price.

B1.2 Any additional services purchased by the Client during the Contract Period shall be detailed on an invoice. This invoice shall be deemed appended to, and form part of, the signed version of this Contract.

B2 Manner of Carrying Out the Services

B2.1 The Supplier shall at all times comply with the Quality Standards, and where applicable shall maintain accreditation with the relevant Quality Standards authorisation body.

B2.2 The Supplier shall ensure that all Staff supplying the Services shall do so with all due skill, care and diligence and shall possess such qualifications, skills and experience as are necessary for the proper supply of the Services.

B3 End of Life Policy

B3.1 Only one version of the IEP software will be available in the market at any one time. Details on the current release functionality is outlined within the User and Administration guides which are available to view and download within the product.

Within the deployed version functional areas may have the following statuses:

B3.1a Validation:

Initial status of new functionality with the overall service, to ensure a controlled introduction to, and feedback from, the market. The customers selected for initial use are decided in cooperation between the Country

Operation's or Partner's deployment organizations, Product Management, Product Support/Development and the Roll-Out Manager.

B3.1b General Availability

When sufficient feedback has been received from the field, as well as from internal stakeholders (deployment, support, product support), the new functionality will either be made Generally Available (GA) or be withdrawn. When made Generally Available each Country Operation/Partner organization can select customers for deployment independently.

B3.1c End of Full Support ("Limited Support Phase")

Institutions will be made aware of the planned withdrawal of a specific functional area within the service. Software updates (patches) will only be made for patient critical defects. Product Support will investigate software issues, but potential non-patient critical fixes will not be made.

B3.1d End of Life

Institutions will be made aware in advance of the end of life date for a functional service element, after which the functionality will be withdrawn.

B4 Business Continuity

B4.1 In the event that the IEP is unavailable, necessary data transfers shall be facilitated by the Client by following the traditional removal encrypted media or printed hard copy processes which must be maintained and securely stored by all participating organisations.

B5 Supplier's Staff

B5.1 The Supplier shall comply with Staff Vetting Procedures in respect of all persons employed or engaged in the provision of the Services.

C PAYMENT AND CONTRACT PRICE

C1 Contract Price

C1.1 Within 5 working days of the Effective Date the Client will provide to the Supplier a valid purchase order.

C1.2 The Supplier will invoice the Client in accordance with the Contract Price plus VAT.

C1.3 The Client shall pay the invoice in accordance with clause C2 (Payment and VAT).

C2 Payment and VAT

C2.1 The Client shall pay all sums due to the Supplier within 30 days of Receipt of a valid invoice. Any overdue payment shall be subject to an interest rate of 1% per month on the invoiced amount.

C2.2 The Supplier shall ensure that each invoice contains all reasonably appropriate references to substantiate the invoice. The Supplier shall add VAT to the Contract Price at the prevailing rate as applicable.

C2.3 Supplier reserves the right to pass on any additional taxes as may be levied by the UK Government from time to time.

C3 Price adjustment on extension of the Initial Contract Period

C3.1 The Contract Price set out in Schedule Two shall apply for the Initial Contract Period. In the event that the Client agrees to extend the Initial Contract Period pursuant to clause F4 (Extension of Initial Contract Period) the Supplier reserves the right to vary the Contract Price.

C3.2 Any variation in the Contract Price will take effect from the first day of any period of extension and shall apply during such period of extension.

D. STATUTORY OBLIGATIONS AND REGULATIONS

D1 Discrimination

D1.1 None of the Parties shall unlawfully discriminate either directly or indirectly on such grounds as race, colour, ethnic or national origin, disability, sex or sexual orientation, religion or belief, or age and without prejudice to the generality of the foregoing none of the Parties shall unlawfully discriminate within the meaning and scope of the Equality Act 2010, the Human Rights Act 1998 or other relevant or equivalent legislation, or any statutory modification or re-enactment thereof.

D2 The Contracts (Rights of Third Parties) Act 1999

D2.1 The Contracts (Rights of Third Parties) Act 1999 shall not apply to this Contract and no person other than the Parties shall have any right under it, nor shall it be enforceable under that Act by any person other than the Parties to it.

E PROTECTION OF INFORMATION

E1 Data Protection

E1.1 Refer to Appendix A

E2 Confidential Information

E2.1 Except to the extent set out in this clause E2 or where disclosure is expressly permitted elsewhere in this Contract, each Party shall:

(a) treat the other party's Confidential Information as confidential; and

(b) not disclose the other party's Confidential Information to any other person without the owner's prior written consent.

E2.2 Clause E2.1 shall not apply to the extent that:

(a) such disclosure is a requirement of Law placed upon the party making the disclosure, including any requirements for disclosure under the FOIA (Freedom of Information);

(b) such information was in the possession of the party making the disclosure without obligation of confidentiality prior to its disclosure by the information owner;

(c) such information was obtained from a third party without obligation of confidentiality;

(d) such information was already in the public domain at the time of disclosure otherwise than by a breach of this Contract; or

(e) it is independently developed without access to the other party's Confidential Information.

E 2.3 The Supplier may only disclose the Client's Confidential Information to the Staff who are directly involved in the provision of the Services and who need to know the information, and shall use all reasonable endeavours to ensure that such Staff are aware of and shall comply with these obligations as to confidentiality.

E 2.4 The Supplier shall use all reasonable endeavours to procure that the Staff do not, use any of the Client's Confidential Information received otherwise than for the purposes of the Contract. With the exception of anonymised data for statistical analysis.

E 2.5 Nothing in this clause E2 shall prevent either Party from using any techniques, ideas or know-how gained during the performance of the Contract in the course of its normal business to the extent that this use does not result in a disclosure of the other Party's Confidential Information or an infringement of either Party's Intellectual Property Rights.

E 2.6 The provisions of this clause E2 shall survive any termination or expiration of the Contract for a period of five years.

E 3 Freedom of Information

E 3.1 The Supplier acknowledges that if the Client is subject to the requirements of the FOIA, the Supplier shall assist and cooperate with the Client to enable the Client to comply with its Information disclosure obligations.

E 3.2 The Supplier shall and shall use all reasonable endeavours to procure that any sub-contractors shall transfer to the Client all Requests for Information that it receives as soon as practicable;

(a) provide the Client with a copy of all Information in its possession, or power in the form that the Client requires as soon as practicable; and

(b) provide all necessary assistance as reasonably requested by the Client to enable the Client to respond to the Request for Information.

E 3.3 In no event shall the Supplier respond directly to a Request for Information unless expressly authorised to do so by the Client or obligated to do so pursuant to applicable Law.

E 3.5 The Supplier acknowledges that (notwithstanding the provisions of Clause E4) the Client may, acting in accordance with the Secretary of State for Constitutional Affairs Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000 ("the Code"), be obliged under the FOIA Regulations to disclose information concerning the Supplier or the Services.

The Client shall;

a) take reasonable steps to consult with the Supplier in advance of any disclosure:

b) take into account the views of the Supplier;

c) if not able to consult prior to disclosure shall provide the Supplier with the disclosure as soon as possible.

E3.6 The Supplier shall ensure that all Information is retained for disclosure and shall permit the Client to inspect such records as requested from time to time.

E4 Intellectual Property Rights

E 4.1 All Intellectual Property Rights in any Software, other computer programs, guidance, specifications, instructions, toolkits, plans, data, drawings, databases, patents, patterns, models, designs or other material (the "IP Materials"):

(a) furnished to or made available to the Client by or on behalf of the Supplier shall remain the property of the Supplier; and

(b) prepared by the Supplier on behalf of the Client in relation to the performance by the Supplier of its obligations under the Contract shall belong to the Supplier; and

(c) The Client shall ensure that the Client Staff shall not, (except when necessary for the performance of the Contract) without prior written Approval of the Supplier, use or disclose any Intellectual Property Rights in the IP Materials to any other person or third party.

E 4.2 For the Initial Contract Period and any extension agreed by the Parties pursuant to clause F4, the Supplier grants to the Client a non-exclusive licence to use the IEP.

F1 Waiver

F 1.1 The failure of either Party to insist upon strict performance of any provision of the Contract, or the failure of either Party to exercise, or any delay in exercising, any right or remedy shall not constitute a waiver of that right or remedy and shall not cause a diminution of the obligations established by the Contract.

F 1.2 No waiver shall be effective unless it is expressly stated to be a waiver and communicated to the other Party in writing in accordance with clause A3 (Notices).

F 1.3 A waiver of any right or remedy arising from a breach of the Contract shall not constitute a waiver of any right or remedy arising from any other or subsequent breach of the Contract.

F2 Severability

F2.1 If any provision of the Contract is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision shall be severed and the remainder of the provisions of the Contract shall continue in full force and effect as if the Contract had been executed with the invalid, illegal or unenforceable provision eliminated.

F3 Monitoring of Contract Performance

F3.1 The Supplier shall comply with the monitoring arrangements set out in the Service Specification Schedule including, but not limited to, providing such data and information as the Supplier may be required to produce under the Contract.

F4 Extension of Initial Contract Period

F4.1 Subject to clause C3. (Price adjustment on extension of the Initial Contract Period), the Client may extend the Contract for a further period of 12 months. Any extension shall be subject to written notification and provision of a valid purchase order from the Client to the Supplier on not less than 1 (one) Months notice prior to the last day of the Initial Contract Period.
The provisions of the Contract will apply (subject to any Variation or adjustment to the Contract Price pursuant to clause C3 (Price adjustment on extension of the Initial Contract Period)) throughout any such extended period.

F5 Entire Agreement

F 5.1 The Contract constitutes the entire agreement between the Parties in respect of the matters dealt with therein. The Contract supersedes all prior negotiations between the Parties and all representations and undertakings made by one Party to the other, whether written or oral.

F 5.2 In the event of, and only to the extent of, any conflict between the clauses of the Contract, any document referred to in those clauses and the Schedules, the conflict shall be resolved in accordance with the following order of precedence:

(a) Contract Change Notice (CCN (if applicable));

(b) the clauses of the Contract;

(b) the Schedules; and

(c) any other document referred to in the clauses of the Contract.

F6 COUNTERPARTS

F6.1 This Contract may be executed in counterparts, each of which executed and delivered shall constitute an original but all counterparts together shall constitute one and the same instrument.

G LIABILITIES

G1 Liability, Indemnity and Insurance

G1.1 Neither Party excludes or limits liability to the other Party for:

(a) death or personal injury caused by its negligence; or

(b) fraud; or

(c) fraudulent misrepresentation; or

(d) any breach of any obligations implied by Section 2 of the Supply of Goods and Services Act 1982.

G1.2 The Supplier shall not be responsible for any injury, loss, damage, cost or expense if and to the extent that it is caused by the negligence or wilful misconduct of the Client or by breach by the Client of its obligations under the Contract.

G1.3 Subject always to clause G1.1 and clause G1.2, the liability of either Party for Defaults shall be subject to the following financial limits:

(a) the aggregate liability of either Party for all its Defaults resulting in direct loss of or damage to the property of the other under or in

connection with the Contract shall in no event exceed the value of the Annual Service Charge paid or payable by the Client; and

(b) the annual aggregate liability under the Contract of either Party for all its Defaults (other than a Default governed by clauses E4 (Intellectual Property Rights), C1.1 and C1.2 (Payment and Contract Price) or G1.3(a) shall in no event exceed the annual Contract Price.

G1.4 Subject always to clause G1.1, in no event shall either Party be liable to the other for any:

(a) loss of profits, business, revenue or goodwill; and/or

(b) loss of savings (whether anticipated or otherwise); and/or

(c) indirect or consequential loss or damage.

G1.5 The Supplier shall effect and maintain with a reputable insurance company a policy or policies of insurance providing an adequate level of cover in respect of all risks which may be incurred by the Supplier, arising out of the Supplier's performance of its obligations under the Contract, including death or personal injury, loss of or damage to property or any other loss. Such insurance shall be maintained for the duration of the Contract Period.

G1.6 The Supplier shall hold employer's liability insurance in respect of Staff in accordance with any legal requirement from time to time in force.

H DEFAULT AND TERMINATION

H1 Termination on insolvency

H1.1 The Client may terminate the Contract with immediate effect by notice in writing to the Supplier where, in respect of the Supplier:

(a) a proposal is made by the Supplier for a voluntary arrangement within Part I of the Insolvency Act 1986 or of any other composition scheme or arrangement with, or assignment for the benefit of, its creditors; or

(b) a shareholders' meeting is convened at which a resolution for its winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation); or

(c) a petition is presented for its winding up (which is not dismissed within 90 days of its service) or an application is made for the appointment of a provisional liquidator or a creditors' meeting is convened pursuant to section 98 of the Insolvency Act 1986; or

(d) a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets; or

(e) an application order is made by the Supplier either for the appointment of an administrator or for an administration order, or an administrator is appointed; or

(f) it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986; or

(g) any event similar to those listed in H1.1(a)-(f) occurs under the law of any other jurisdiction.

H2 Termination on Default or by Notice

H 2.1 Either Party may terminate the Contract by written notice to the other Party with immediate effect if the other Party commits a Default and if:

(a) the defaulting Party has not remedied the Default to the reasonable satisfaction of the terminating Party within 30 Working Day, after issue of a written notice specifying the Default and requesting it to be remedied; or

(b) the Default is a material breach of the Contract.

H 2.2 If the Client fails to pay the Supplier any sum of money when due, the Supplier shall notify the Client in writing of such failure to pay. If the Client fails to pay such sum within 30 Working Days of the date of such written notice, the Supplier may terminate the Contract in writing with immediate effect.

H.2.3 Without prejudice to any rights that have accrued under the Contract and/or other any rights or remedies available to the relevant Party, if the Contract is extended pursuant to clause A2 or F4, either Party may terminate this Contract at any time after the Initial Contract Period by giving 6 months written notice to the other Party. No part of any Contract Price already paid will be refundable.

H3 Consequences of Termination on Insolvency

H 3.1 Where the Client shall be entitled to terminate the Contract under clause H1 (Termination on Insolvency) and does so terminate in accordance with clause H1.1,the Supplier will cooperate with the Replacement Supplier to ensure the orderly transition of the services similar to or identical to the Service.

H 4 Force Majeure

H 4.1 Neither Party shall be liable to the other Party for any delay in performing, or failure to perform, its obligations under the Contract (other than a payment of money) to the extent that such delay or failure is a result of Force Majeure. Notwithstanding the foregoing, each Party shall use all reasonable endeavours to continue to perform its obligations under the Contract for the duration of such Force Majeure. However, if such Force Majeure prevents either Party from performing its material obligations under the Contract for a period in excess of six Months, either Party may terminate the Contract with immediate effect by notice in writing.

H 4.2 Any failure or delay by the Supplier in performing its obligations under the Contract which results from any failure or delay by an agent, sub-contractor or supplier shall be regarded as due to Force Majeure only if that agent, sub-

contractor or supplier is itself impeded by Force Majeure from complying with an obligation to the Supplier.

H 4.3 If either Party becomes aware of Force Majeure which gives rise to, or is likely to give rise to, any failure or delay on its part as described in clause H4.1 it shall immediately notify the other by the most expeditious method then available and shall inform the other of the period for which it is estimated that such failure or delay shall continue.

H 5 Clauses of this agreement to survive termination

H5.1 All clauses of the Contract which by their nature are intended to survive any termination or expiration of this Contract, including clause E2 (Confidential Information) as explicitly set forth in clause E2.6, shall survive such termination or expiration.

I DISPUTES AND LAW

I 1 Governing Law and Jurisdiction

Subject to the provisions of clause I2, the Client and the Supplier accept the exclusive jurisdiction of the English courts and agree that the Contract and all non-contractual obligations and other matters arising from or connected with it are to be governed and construed according to English Law.

I 2 Dispute Resolution

I 2.1 The Parties shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with the Contract within 20 Working Days of either Party notifying the other of the dispute and such efforts shall involve the escalation of the dispute to the managing director (or equivalent) of each Party.

I 2.2 Nothing in this dispute resolution procedure shall prevent the Parties from seeking from any court of competent jurisdiction an interim order restraining the other Party from doing any act or compelling the other Party to do any act.

I 2.3 If the dispute cannot be resolved by the Parties pursuant to clause I2.1 the Parties shall refer it to mediation unless (a) the Client considers that the dispute is not suitable for resolution by mediation; or (b) the Supplier does not agree to mediation.

I 2.4 The obligations of the Parties under the Contract shall not cease or be suspended or delayed by the reference of a dispute to mediation (or arbitration) and the Supplier and the Staff shall comply fully with the requirements of the Contract at all times.

.

Appendix A

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is entered on the , by and between

(hereinafter referred to as "Controller")
and
Sectra Limited Company Reg No. 4571654, (hereinafter referred to as "Processor")

The Processor and Controller are hereinafter referred to separately by "Party" and jointly by the "Parties".
WHEREAS
This DPA supplements any agreement (Main Agreement) between the Parties that requires Processing of Personal Data. In the event of conflicting provisions, this DPA shall only take precedence regarding Processing of Personal Data.

1. DEFINITIONS

1.1. The definitions used in GDPR are applicable in this DPA. For ease of use of this DPA a few of the GDPR definitions are listed below (if they should differ to the definitions in the GDPR the definitions in the GDPR applies):

1.1.1 "Controller" means 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; where the purposes and means of such Processing are determined by Union or Member State law, the Controller or the specific criteria for its nomination may be provided for by Union, Member State or UK law;

1.1.2 "Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, 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;

1.1.3 "Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

1.1.4 “Processor” means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller;

1.1.5 “Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed;

1.2 In addition to the definitions in GDPR the following definitions shall be applicable in this DPA;

1.2.1 ”Applicable Laws" means any applicable law relating to the processing, privacy and use of Personal Data, as applicable to either party of the services under this agreement, including the Data Protection Act and/or the GDPR, and /or any corresponding or equivalent national laws or regulations; and any laws which implement such laws; and any laws that replace, extend, re-enact, consolidate or ament any of the foregoing; all guidance, guidance, codes of practice and codes of conduct issued by the Information Commissioner or any relevant regulator, authority or body responsible for administering Data Protection legislation (in each case whether or not legally binding);

1.2.2 “GDPR” means the UK GDPR as defined in sections 3(10) and 205 (4) of the Data Protection Act 2018

1.2.3 "Services" means the services and other activities to be supplied to or carried out by or on behalf of Processor for Controllers pursuant to the relevant agreements between the Parties; and

1.2.4 "Subprocessor" means any Third Party, though excluding employees of the Processor or employees of any of its Subprocessors, appointed by or on behalf of the Processor to Process Personal Data on behalf of the Controller to perform the Services.

1.2.5 “Supervisory Authority” means the Information Commissioner’s Office.

2. PROCESSING OF PERSONAL DATA

2.1 The Controller shall ensure that:

2.1.1 the processing of Personal Data, including transfer of Personal Data to the Processor, will be carried out in accordance with the relevant provisions of the Applicable Laws and, where applicable by law, has been notified to the relevant authorities of the country where the Personal Data is processed;

2.1.2 it will throughout the duration of the Personal Data processing services only instruct Processor to process the Personal Data in accordance with the Applicable Laws and this agreement; and

2.1.3 it has implemented technical and organisational security measures in accordance with Applicable Laws before processing the Personal Data and such technical and organisational security measures are regularly updated.

2.2 Processor may only Process Personal Data in compliance with Applicable Laws, this DPA and in accordance with written instructions from the Controller in Appendix 1, and relevant agreements between the Parties. Processor may not process Personal Data for any purpose other than those specified by Controller.

2.3 The Processor shall, if requested by the Controller, inform the Controller where Personal Data is processed and transferred.

2.4 The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes any Applicable Laws.

2.5 The Processor shall assist the Controller by appropriate technical and organisational measures, insofar as possible and taking into account the nature of the Processing and the information available to the Processor, in fulfilling the Controller's obligations under Applicable Laws with regards to request from Data Subjects, and general privacy compliance under Article 32 to 36 of the GDPR.

2.6 Processor shall:

2.6.1 comply with all Applicable Laws in the Processing of Personal Data; and

2.6.2 Process Personal Data in accordance with relevant Controller's documented instructions unless Processing is required by Applicable Laws to which the relevant contracted Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform the relevant Controller of that legal requirement before the relevant Processing of that Personal Data.

2.7 Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know and have access the relevant Personal Data, as strictly necessary for the purposes of this DPA and any relevant agreement between the Parties, and to comply with Applicable Laws, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

3. Transfer to a third country

3.1 The Processor may only transfer Personal Data to countries that have an adequate level of protection, though the Processor may transfer Personal Data to a third country, that does not have an adequate level of protection, if the Processor has provided appropriate safeguards, and on condition that enforceable Data Subject rights and effective legal remedies for data subjects are available, in accordance with Article 46 of the GDPR.

3.2 If transfer of Personal Data to a third country requires an agreement with standard contractual clauses approved by European Commission for the transfer of Personal Data the Processor is responsible for the execution of such an agreement for the purpose of maintaining an adequate level of protection of Personal Data before any transfer of Personal Data is performed.

4. SUBPROCESSOR

4.1 The Processor does not have the right to designate Subprocessors for the Processing of Personal Data under this DPA, without informing the Controller. Before the Processor designates any new Subprocessor, the Processor shall provide the Controller with the following information: a) who the Subprocessor is, including its contact information, company formation type and geographic location; b) what kind of service the Subprocessor is providing; c) the measures taken to ensure that the Subprocessor complies with the Applicable Laws; and d) the geographic location(s) where the Subprocessor Processes Personal Data covered by this DPA. The Processor shall ensure that each Subprocessor is under the same or stricter obligations than this DPA.

4.2 The Controller and Processor are entitled to terminate this DPA and any agreement (Main Agreement) between the Parties that is dependent of the Processor's Processing of the Controller's Personal Data if the Controller objects to a Subprocessor. The termination period will be according to the termination clauses included in the Main Agreement. If there are no termination clauses in the Main Agreement the termination period will be four (4) months.

4.3 The Subprocessors in Appendix 1 are approved by the Controller.

4.4 The Processor shall ensure that Subprocessors agree to undertake responsibilities corresponding to the obligations set out in this DPA. The Processor shall ensure that each Subprocessor is under the same or stricter obligations than this DPA. The Processor accepts full liability for the Subprocessors' Processing of the Controller's Personal Data.

5. AUDIT

5.1 During the term of this DPA, the Controller and any Supervisory Authority shall be entitled to, by itself or through a representative at its own cost, audit

the Processor and any Subprocessor to verify that the Processor complies with the requirements set forth in this DPA and Applicable Laws up to once a year. The Processor shall at any time requested by the Controller, subject to a four (4) weeks written notice by the Controller, and at the Processor's own expense, submit its data processing facilities, records, data files and documentation needed for Processing of the Controller's Personal Data to be audited by the Controller (or any Third Party such as inspection agents or auditors, selected by Controller) to ascertain compliance with this DPA and Applicable Laws. The Processor shall assist the person(s) performing the audit with access to documentation, premises, IT systems and other assets necessary to monitor compliance. The Processor shall also ensure that Controller has the corresponding rights in relation to any Subprocessor. The Parties may agree on alternative follow-up procedures, such as reviews conducted by independent Third Parties.

5.2 In any case, audits must be conducted during regular business hours at the applicable facility, subject to the Processors policies, and may not unreasonably interfere with the Processor's business activities.

6. PERSONAL DATA BREACH

6.1 The Processor shall notify the Controller in writing, without undue delay, if the Processor or any of its Subprocessors becomes aware of a Personal Data Breach affecting Personal Data, for example but not limited to unauthorized Processing, unauthorized access, destruction or alteration of Personal Data, as well as attempts to such activities. The Processor shall provide the Controller with sufficient information to allow the Controller to meet any obligations to report or inform Supervisory Authority or Data Subjects of the Personal Data Breach under the Applicable Laws and in particular Article 33 of the GDPR.

6.2 Notifications of Personal Data Breaches shall be sent to:

The Controller should send a confirmation e-mail to the Processor to inform that the breach notification has been received.

6.3 The Processor shall cooperate with the Controller and take such reasonable steps as directed by the Controller to assist in the investigation, mitigation and remediation of each Personal Data Breach.

6.4 The Processor shall document any Personal Data Breaches, comprising the facts relating to the Personal Data Breach, its effects and the remedial action taken. This documentation shall enable the Controller to verify compliance with this DPA and Applicable Laws.

7. SECURITY, SAFETY MEASURES AND DATA SUBJECT RIGHTS

7.1 The Processor is aware of the importance of data protection by design and by default. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purpose of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall in relation to the Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including but not limited to, as appropriate, the measures referred to in Article 32(1) of the GDPR.

7.2 In assessing the appropriate level of security, the Processor shall consider the risks of Processing the Personal Data and in particular, risks for Personal Data Breaches.

7.3 The Processor shall in writing inform the Controller of any material, technical or organizational changes to the Processing of Personal Data if the changes can negatively affect the security of the Processing.

7.4 If the Processor or its Subprocessors make technical changes and in particular are using new technologies, and taking into account the nature, scope, context and purpose of the Processing, that is likely to result in a high risk to the rights and freedoms of natural persons, the Processor shall, prior to the Processing, notify the Controller so that the Controller can carry out an assessment of the impact of the envisaged Processing operations on the protection of Personal Data in accordance with Article 35 and 36 of the GDPR.

7.5 The Processor shall provide and implement technical and practical measures to investigate any suspicion that a person has or has had unauthorized access to Personal Data.

7.6 The Processor shall promptly notify the Controller about:

a) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

b) any request received directly from Data Subjects without responding to that request, unless it has been otherwise authorised to do so by the Controller or Supervisory Authority;

7.7 The Processor shall assist the Controller, insofar as possible and considering the nature of the Processing and the information available to the Processor, in fulfilling the Controller's obligations with regards to request from Data Subjects. The Controller shall use normal work order procedures when requesting assistance for this.

8. Notices

8.1 All notices, requests, demands, approvals, waivers and other communications required or permitted under this Data Processing Agreement must be in writing and shall be deemed to have been received by a Party when:

(a) delivered by post, unless actually received earlier, on the third Business Day after posting;

(b) delivered by hand, on the day of delivery;

(c) delivered by e-mail, upon confirmation by the receiving Party.

8.2 All such notices and communications shall be addressed as set out in this DPA or to such other addresses as may be given by written notice in accordance with this clause.

9. INDEMNITY

9.1 If any of the Parties breaches applicable Laws and the non-breaching Party must pay any compensation or any administrative fines to any third party for such breach, including any Data Subject or Authority, due to such breach the breaching Party shall remunerate the non-breaching Party for such compensation and administrative fines.

10. SEVERANCE

10.1 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

11. Amendments

11.1 Only those amendments and additions to this DPA that are made in writing and signed by the Parties are valid.

12. TERM AND TERMINATION

12.1 This DPA is valid as long as the Processor processes Personal Data on behalf of the Controller. The DPA will be automatically terminated when the Parties' agreement that require the Processing of Personal Data is terminated or expires. Upon termination of the DPA or when the Processor and its Subprocessors are no longer authorized to process any of the Controller's Personal Data the Processor shall at the request of the Controller ensure that all Personal Data is transferred to the Controller in a machine-readable format, in line with the exit plan within the Main

Agreement, or, if such a plan doesn't exist, within three (3) months from such request. The Controller may also request that the Processor deletes all Personal Data that has been processed under this DPA within thirty (30) days after the transfer of the Personal Data to the Controller, and confirm this to the Controller in writing unless required to keep certain Personal Data to comply with applicable laws whereas the Processor in writing shall inform the Controller of which Personal Data that will be retained.

12.2 The Processor may only retain Personal Data after termination of the DPA, to the extent it is required by law, subject to the same type of technical and organisational security measures as outlined in this DPA.

13. GOVERNING LAW AND JURISDICTION

13.1 This Agreement is subject to the governing law, jurisdiction and legal venue as set out in the agreement (Main Agreement) between the Parties that requires Processing of Personal Data.

***

Appendix 1

Instructions for data processing

These instructions are an integral part of the Data Processing Agreement (DPA) and shall be followed by the Processor in the performance of personal data processing, unless expressly stated in the Data Processing Agreement. By signing the Data Processing Agreement, the Processor has confirmed these instructions. All changes and additions to these instructions shall be in writing to be valid.

Purpose

Specify the purposes for which Personal Data will be processed by the Processor.

Electronic Transmission of Health Images and Reports

Processing

Specify the Processing activities that will be performed by the Processor:

Electronic transmission of Health records and analysis of data and log files to solve support and service questions and to perform maintenance as well as product enhancements.

Type of Personal Data

Specify the type of Personal Data that will be processed by the Processor:

Name, Address, Data of Birth, Email Address, Telephone Number, IP Address, Medical Images and Reports.

Category of Data Subjects

Specify which categories of Data Subjects the Processor will process personal data about:

Patients and referring physician.

Location of Processing

Specify all geographic locations where the personal data will be processed by the Processor:

England and Sectra Support Offices within the EEA.

Technical and organisational measures

Specify the technical and organisational measures that must be in place to protect the Personal Data

Encryption and ISO 27001 implementation (full scope)

Transfer to third countries

If applicable, state whether Personal Data is transferred, directly or indirectly,
to a country/state outside of the EU/EEA and the safeguards in place to protect the Personal Data.

Not applicable

Approved Subprocessors

Company name & company formation type	Address and contact information	Processing services	Geographic location of the Processing service(s)	Security and legal measures
N/A	N/A	N/A	N/A	N/A

Schedule One - Service Specification Schedule and Connection Agreement

Related Documents

Document Reference Number	Document Title	Approved Version
[1]	NHS Data Security and Protection Toolkit	Current
[2]	Internet First Policy and Guidance	Current
[3]	Data Protection Act 2018	Current
[4]	General Data Protection Regulation	Current

Definitions

Term	Definition
Applicable Laws	means any applicable law relating to data protection and security, including without limitation Data Protection Act 2018 and the UK GDPR (as defined in sections 3(10) and 205(4) of the Data Protection Act 2018)
Enablement Form	means the document of Client's acceptance for the service to go-live
Fault	means a problem with the operation of the IEP service
Multidisciplinary Team Meeting	a meeting of a group of professionals from one or more clinical disciplines who together make decisions regarding recommended treatment of individual patients.
Personal Data	means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, 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
Receiving Organisation	the organisation within which data is to be received or where users have been granted access to the IEP web viewer

IEP SERVICE DESCRIPTION

The Image Exchange Portal (IEP) enables the secure exchange of diagnostic images, reports and other clinical data between organisations which are connected to it; using open standard DICOM and HL7 protocols through a secure encrypted VPN running over N3/HSCN or the internet.

The exchange of patient data is initiated and managed using a secure web-based application and the exchanges of patient data are defined in terms of Transactions.

PRE-REQUISITES OF CONNECTING TO IEP

Each organisation connecting to IEP will have in place:

- Imaging Transfer Request Policy and Procedures – These should define how a user may request the import or export of Images and reports to or from their organisation. These must include detail of how the IEP and any supplementary mechanisms will be used for, Internal Imaging Transfer Requests, External Imaging Transfer Request and External Imaging Transfer Notifications.

- Multi-disciplinary Team Meeting (MDTM) Policy and Procedures (if applicable) – These should define the processes associated with the referral to and running of an MDTM, it is assumed that these will be in line with the Royal College of Radiology guidance.

- Harmonisation Governance - Where the IEP is to be used to manipulate data such as DICOM headers, in order to harmonise data on import to the receiving organisation's PACS, that organisation must establish an appropriate review and approval processes to set up the original harmonisation rules and to add or edit the harmonisation rules on an ongoing basis.

- A valid NHS Digital Data Security and Protection Toolkit [1] submission with a status of "Standards Met". This will be maintained annually in line with NHS Digital requirements.

OUT OF HOURS AND BUSINESS CONTINUITY

All organisations connected to IEP must ensure that they review the out of hours requirement for data sharing within their organisation to ensure that IEP is configured appropriately and that relevant staff are available to access, operate and support the IEP service.

In the event that the IEP solution is unavailable, organisations using IEP must ensure that they have processes in place to ensure necessary data transfers shall be facilitated by following the existing removable media or printed hard copy processes which must be maintained and securely stored by all organisations utilising the IEP service.

PATIENT CONSENT

Patient consent is required for data sharing between legal organisations, unless shared as part of a patient care referral. In addition, all authorised users are required to have a legitimate relationship and reason to access a patient's data.

There is currently no technical solution to restrict access in line with requirements for patient consent and legitimate relationships. In this situation data sharing may be permitted on an informed implied consent model within a policy framework that appropriately restricts access to those with a legitimate reason to access shared data.

As the system and its users cannot tell if a patient has consented to sharing their data, it is assumed that all data on the IEP may potentially be shared with a user in a different organisation. All participating organisations must therefore have in place policies and procedures to inform patients how and why their data will be shared unless they dissent, how their dissent will be acted upon, and what the consequences of a decision to dissent are.

ONWARD TRANSFERS

It is the responsibility of the Receiving Organisation to ensure that data will be treated in accordance with this Contract and Applicable Laws.

AUDIT LOGS

The IEP system retains an audit log of all transactions undertaken and contains activity data by organisation, user, time and information type and the data used to generate the audit trail is stored in the database by the IEP application. Transaction history is retained for 28 days.

System audit logs are retained for 7 years, with the most recent 12 months being accessible through the IEP web interface.

Each event is captured and linked to other tables in the database to build up a comprehensive set of audit data for Information Governance, user administration and system analysis. The audit data presented to the user is a read only view of the selected fields from the audit database.

Only an authorised User from each IEP Institution can access the System Audit Information screen. They are able to filter the events by Action (event type), Study (Accession number), user or patient. By using a combination of patient name and date of birth, all events relating to an individual patient can be shown irrespective of the Patient IDs used.

All events will have a date and time stamp, the service involved, the name of the event, the user and their current logged in institution.

SERVICE LEVELS

Upon signing of the Enablement Form (within the project documentation) the following service levels apply.

IEP SERVICE AVAILABILITY

Subject to the provisions of this Schedule One, in particular and without limitation to the Client observing it's roles and responsibilities described below, the Supplier shall endeavour to operate the IEP Service on a 24 x 7 x 365 days per year basis. The Supplier will target an up time of 98% of the IEP Service (excluding any downtime caused by issues beyond the Suppliers' control including network connectivity and continuity of service).

By signing up to IEP each organisation recognises that the transfer times to and from IEP are dependent upon the bandwidth availability on the Internet and/or N3/HSCN network end-to-end. As a consequence, and in line with all image transfer solutions using the Internet and/or N3/HSCN, although the performance of the IEP will be monitored by the service provider (Sectra), the response and delivery times cannot be guaranteed.

The initiator can only send to users eligible to receive the transaction from a drop-down list. This list of potential recipients is set by the organisation(s) and group(s) they belong to and the individual privileges for those organisations. Once authenticated, the user will be allocated the roles and privileges assigned to them by the institution they have logged into[1].

The Supplier shall perform the following under the Contract:

1. Service monitoring – Every effort will be made to conduct periodic monitoring of the performance and availability of the Services and in particular, to the extent that the Supplier shall be reasonably able to procure the same.

2. Infrastructure monitoring – Every effort will be made to conduct periodic monitoring of the performance and availability of the Service infrastructure to include; network, hardware and resources.

3. Preventative maintenance – Every effort will be made to identify, analyse and prevent potential problems that could impact the availability of the Services.

4. Service Support – The Supplier Helpdesk will provide support to the Client (within the operating hours stated below) in relation to the Services and the supporting infrastructure within the control of the Supplier.

5. Problem Ticket recording - The Supplier Helpdesk will securely record all help requests within a suitable record management system and supply the Client with a ticket number to enable suitable tracking of the help request.

6. Knowledge Management – The Supplier will use the recording, storage and retrieval of information to assist in the resolution of problems raised.

[1] A user may belong to multiple organisations and use the same user ID to access the IEP.

HELP DESK

The Client shall be responsible for notifying the Supplier Help Desk of Faults within the "Core Hours" as defined below.

Core Hours: Monday – Friday 09.00 – 17.30

Helpdesk phone number: +44 (0) 800 29 22 066
Helpdesk email: iephelpdesk@sectra.com

Between the hours of 08.00 - 09.00 and 17.30 to 20.00 Monday to Friday and 09.00 - 13.00 Saturday, Sunday and Bank Holidays the Helpdesk operates an on-call service for severity level 1 Faults only. These must be telephoned through to the Helpdesk.

Each Fault or problem will be recorded by the Supplier in the form of an incident and the Client will be informed of the reference number associated with each incident. Each incident will be allocated a severity level in accordance with the table below ("Severity Level").

Severity Level	Definition
1	This classification indicates a major incident, loss of Service or serious impairment of Service which cannot be immediately circumvented. Examples are: • Inability to transfer any [DICOM] studies to and from the IEP Service
2	This classification indicates an issue that is not a major service affecting Fault, and generally constitutes a failure of a component of a Service, which does not have a significant impact on the service as a whole. Example: • Single element of the system breaches, but system continues to work.
3	This classification indicates an issue that is not service affecting. Examples are: • Request for support • Request for information

TARGET RESOLUTION TIMES

Where a Fault is established, the Supplier will attempt to rectify the Fault or provide a workaround within the Target Resolution Times allocated to each Severity Level, as described below, whenever possible.

Severity Level	Target Resolution Time
1	Resolve within 4 hours
2	Resolve within 2 Working Days
3	Resolve within 5 Working Days

For the purposes of the Target Resolution Time no account shall be taken of any period falling outside the Core Hours of the Helpdesk, except in the event of a Severity Level 1.

ROLES AND RESPONSIBILITIES

The **Client** will observe and perform its responsibilities as detailed below:

- To conduct business in a courteous and professional manner with the Supplier.
- Ensure the Services are used as is intended under the Contract.
- Ensure a suitable VPN is available, configured and maintained with sufficient bandwidth for data and image transfers to complete successfully.
- Have in place a valid NHS Digital Data Security and Protection Toolkit[1] submission with a status of “Standards Met” and ensure this is maintained annually per NHS Digital’s requirements.
- Adhere to Internet First Policy and Guidance [2]
- Process Personal Data in accordance with the Data Protection Act 2018 [3] and General Data Protection Regulation (GDPR) [4]
- Have in place and maintain, having regard to the state of technological development and the cost implementation, all appropriate measures , procedures and policies to protect the confidentiality, availability and integrity of Personal Data.
- Ensure that all staff utilising IEP will have the necessary Information Security training and follow this Agreement.
- Have a lawful basis for sharing data over IEP
- Ensure the Caldicott Guardian or an authorised representative approves IEP information flows for their Institution.
- The Client’s Service users will only use the Supplier Helpdesk to request support in accordance with this Schedule One.
- Use the appropriate internal Client helpdesk support services for local network, firewall, smartcard and infrastructure issues.
- Provide all information to the Supplier which it requires to open a support ticket.
- Once a support ticket has been submitted, the Client will make itself available to work with the Supplier’s support resource allocated to the support ticket.
- Will be responsible for the proper configuration of all equipment at the Client’s site for the Services.
- The Client will be responsible for ensuring all Information Governance requirements and procedures are met by its staff.
- The Client undertakes not to use the Services for the transfer of Personal Data outside of the EEA unless permitted by Law.

- The Client undertakes to maintain a suitable business continuity plan which would cover the loss of services as detailed in Schedule One.

The **Supplier** has the following general responsibilities under this Contract:

- To conduct business in a courteous and professional manner with the Client
- Notwithstanding any other provision of the Contract, the Supplier will endeavour to ensure the availability of the Services to the Client but due to the nature of the Services, reliability of 3rd party links and reliance of information supplied by the Client, the Supplier cannot guarantee the Services will be provided within any particular time or at any particular level.
- Ensure the security of the Services and that patient data is securely maintained during its transfer or utilisation on the Services and conformance at all times to NHS information governance standards and guidelines.
- When the Client reports a problem with the Services, the Supplier will record all information provided by the Client required to document the nature of the problem.
- Assign severity codes adhering to the correct usage as detailed above.
- Endeavour to resolve problems within the Target Resolution Times detailed above subject to the Service Limitations.
- Escalate support requests to the next level of internal support upon approach of established Target Resolution Times.
- Liaise with any appropriate Client helpdesk to aid the resolution of a problem that affects the ability of the Client to use the Service.
- Communicate to the Client the status of a ticket at reasonable intervals to be determined by the severity level and the Supplier Helpdesk support resource.
- Obtain the Client's approval (which shall not be unreasonably withheld or delayed) before ticket closure.

Schedule Two - Pricing & Payment Terms

Service Description	Set up	Annual Service Charge (subject to review in accordance with clause C3)

Please Note –

All costs exclude VAT, which will be charged at the standard rate

Setup Costs include the initial configuration of the service; the set up cost includes a Training Session for a maximum of 4 delegates. Training is supplied on a "Train the Trainer" basis and is held on Client premises, Sectra premises or Remote Training Session. The Client is responsible for providing a suitable training room for the training to take place. Any additional training requirements beyond the initial session will be charged at the prevailing daily rate for an Applications Specialist.

Payment for the IEP service is annually in advance. The IEP Services charge will be invoiced at the point of the Commencement Date.

An annual service charge for subsequent use of the IEP Services will be invoiced one month prior to the end of the Initial Contract Period as a condition precedent to the continuation of the Services for a further twelve months.

The minimum commitment use of the IEP service is 12 months.

Payment in full by the Client to the Supplier of the relevant annual service charge is a mandatory requirement of it maintaining connection to IEP and receiving the Services.

Volume Based Pricing

The IEP Annual Service Charge is calculated by measuring the annual volume of transactions 2 months prior to the contract expiry date. Transaction volume levels will be measured to determine the pricing tier and a renewal notification sent informing the trust of the price for the next 12 months.
Each standard transaction (IEP Institution to IEP Institution) will count as 1 towards the annual volume count.
IEP with Anyone Transfers (IEP Institution to non IEP connected end users) will be counted as follows:
15 Day Retention Period will count as 5 towards the annual volume count.
30 Day Retention Period will count as 6 towards the annual volume count.
60 Day Retention Period will count as 8 towards the annual volume count.

The volume measured is institution specific and is the sum of the total number of inbound and outbound transactions. Each transaction can contain one or more studies (which can contain multiple images) for a specific patient.

Pricing Tiers

Transactions < than	Charge
500	£
10,000	£
25,000	£
50,000	£
100,000	£
150,000	£
200,000	£
300,000	£
400,000	£
500,000	£