Data Sharing Agreement

BETWEEN

All West Kent GP Practices (list at appendix 1)

AND

Hospice in the Weald (West Kent)

(Hereinafter known as the Joint Controllers)

In Support of data sharing of patients' data via EMIS/Vision clinical system to provide end of life palliative care

Version History	1.0
Created By	GP DPO team Kent and Medway CCG
Supported By	The Kent and Medway CCG
Implemented By	All parties
Commencement Date	TBC
Review Date	Every 12 months or as necessary subject to changes in available sharing mechanism or changes in applicable legislations.

1.0 Introduction

1.1. The purpose of this Joint Controller Agreement (the Agreement) is to set out the parameters for the sharing and use of personal health and/or social care data as required for the direct provision of end of life palliative care to patients. The Agreement will cover as applicable, patients and service users under the care of the Hospice in the Weald Nursing, Medical and Therapy Services whose care will be managed across the whole of West Kent. It also sets out how joint control of data is compliant with relevant legal and regulatory requirements.

1.2. The terms and conditions of this Agreement shall apply to all NHS health Information and/or social care data provided by Controllers who are parties to this agreement; or obtained by a Processor to any Controller, party to this agreement from other sources as part of the delivery of the contracted services or derived from any combination thereof.

1.3. This Agreement between the Joint Controllers supports and is specific to sharing personal health and/or social care data for the purposes of providing end of life palliative care in this agreement; and any other supplementary services not specifically stated in this agreement, but which is incidental to providing such care in the West Kent area and/or the discharge of any other stated purposes referred to in any part of this Agreement.

2.0 Background

2.1. Hospice in the Weald Nursing, Medical and Therapy Services provides end of life palliative care services (at Hospices in the Weald and/or within the communities) across the West Kent areas.

2.2 It was previously understood that Hospice in the Weald obtain and share relevant patients' data with Practices via the CPMS system; however, recent feedback indicated this doesn't work, hence the consideration of sharing data via the EMIS clinical system or Vision clinical system if applicable.

2.3 As Hospice in the Weald uses EMIS web and clinical systems; they have requested electronic access to patients' data via EMIS to EMIS sharing. This is a two way sharing that allow both parties to update patients treatment/care plan on their individual systems whilst allowing both parties to read this practically in real time.

2.4 Under the oversight of the CCG leadership team, there has been significant considerations of the appropriateness of data sharing between hospices and practices within Kent and Medway. These include advice sought from Capsticks Solicitors, the ICO, the Office of the National Data Guardian and EMIS clinical system itself; resulting in the approval of data sharing via EMIS clinical system between Kent and Medway Practices and the relevant Hospices in the various local areas as required.

2.5 The approval to share data between the practices and Hospice in the Weald via EMIS clinical system is being agreed subject to some governance controls which are embedded variously within this Agreement. Fuller details are stated in the DPIA, including the justifications and considerations of the proportionality of the patients' data to be shared.

3.0 Definitions

3.1. **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.

3.2. **Special categories of personal data (i.e. sensitive personal data)*** the categories of personal information as defined in the General Data Protection Regulation (GDPR) and the Data Protection

Act 2018 (DPA 2018), 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.

3.3. **Confidential Information*** any information or combination of information that contains details about an individual person that was provided in an expectation of confidence. This includes for example, Personal data about patients, service users and staff.

3.4. **Patient Information*** any patient information under the control of the Controller. This includes all information supplied to a Processor by the Controller and any additional information that a Processor obtains during the term of its data processing contract and shall apply equally to original Patient Information and all back-up and/or copies printed out.

3.5. **Controller*** as defined in the GDPR is the individual or organisation (legal person) who, alone or jointly, determines the manner and purpose of the processing of Personal data, including what information will be processed and how it will be obtained.

3.6. **Joint Controller*** as defined in Article 26 of the GDPR is where two or more Controllers jointly determine the purposes and means of Processing.

3.7. **Care and Support Plan*** the management plan, to be shared with the appropriate MDT members, containing the reason for referral to the MDT; the outcomes of the MDT discussion; and the action points required including an administrative section that details whether the patient is open/closed to the MDT and timescales for discussion

3.8. **Processor*** as defined in the GDPR , is an individual (other than an employee of the Controller) or organisation who processes Personal data on behalf of the Controller, under a data processing contract.

3.9. **Processing*** as defined in the GDPR in respect of Personal data, for the purpose of this Agreement includes any business activity or contracted service involved in the use of Personal data, including obtaining, recording, holding, viewing, storing, adapting, altering, deleting and disclosing. This is not restricted to computer processing, but includes manual files.

4.0 Purpose of Joint Sharing

4.1. The key purpose of joint sharing is:

- To share patients' data between applicable West Kent GP Practice and Hospice in the Weald during the course of providing end of life palliative care via a both ways EMIS to EMIS data sharing; and
- Any other supplementary services not specifically stated in this agreement, but which is incidental to providing such care in the West Kent area and/or the discharge of any other stated purposes referred to in any part of this Agreement.

4.2 Permissions

4.2.1 In order to fulfil the purpose outlined above, parties will be granted access to each other's EMIS Web and/or clinical Care Record in line with permissions outlined below:

EMIS Web Care Record sharing agreement 1 (GP to Hospice)

Agreement Name	**GP's to Hospice in the Weald Nursing, Medical and Therapies**	
Care Record Sharing Agreement details	Shared	View free text

Care Record Summary including Problems, medication, Allergies, Alerts, Recent Activity and Health Status	Yes	Yes
Consultations	Yes	Yes
Medication	Yes	Yes
Problems	Yes	Yes
Investigations	Yes	Yes
History	Yes	Yes
Diary	Yes	Yes
Attachments	Yes	Yes
Referrals	Yes	Yes
Task Box	Yes	Yes
What job categories can view shared data?	All	

EMIS Web Care Record sharing agreement 2 (Hospice to GP)

Agreement Name	Hospice in the Weald Nursing, Medical and Therapies to GP's	
Care Record Sharing Agreement details	Shared	View free text
Care Record Summary including Problems, Medication, Allergies, Alerts, Recent Activity and Health Status	Yes	Yes
Consultations	Yes	Yes
Medication	Yes	Yes
Problems	Yes	Yes
Investigations	Yes	Yes
History	Yes	Yes
Diary	Yes	Yes
Attachments	Yes	Yes
Referrals	Yes	Yes
Task Box	Yes	Yes
What job categories can view shared data?	All	

4.3 The Hospice in the Weald Nursing, Medical and Therapy Services have several departments as follows:

a) The In-Patient Unit
b) Hospice in the Home
c) Hospice Day Service
d) Carer Support Department
e) Complementary Therapies
f) Counselling and Support Services
g) Occupational Therapy
h) Physiotherapy
i) Spiritual Care

5.0 General

5.1. It is important to establish who the Controller of the Personal data is, as Controllers are required to comply with the data protection principles and meet the obligations imposed by the DPA 2018.

5.2. Joint Controllers act together, setting out the shared purposes for Processing, the manner of Processing and how legal obligations and responsibilities will be satisfied. The participation of the Joint Controllers may take different forms and their contributions may be sequential or simultaneous.

5.3. Based on the above definition, if the Parties to this Agreement process jointly for the shared purposes stated, they are Joint Controllers. This Agreement determines their respective responsibilities for compliance with the GDPR and respecting data subject rights (unless required by law to act without such instructions).

5.4. Of note, owing to the setup of the EMIS clinical system, any party (GP practice or Hospices in the Weald) may choose to utilise the EMIS inclusion/exclusion codes to tailor the type of data to be shared. The list of these codes is listed here:

EMIS-GP-Summary-E
xclusion-Code-List.pd

5.5 It is also agreed that once a patient has been referred and Hospices in the Weald has identified the need for further health information of the patient, they would have a process of notifying the patient of this need, their rights and how they can exercise it. This would include their right to object which would be respected.

5.7. Under this Agreement Parties retain the following direct responsibilities:

- To co-operate with supervisory authorities (such as the Information Commissioner's Office);
- To ensure the security of processing;
- To keep records of processing activities;
- To notify any Personal data breaches to each Controller, and if applicable, to the Information Commissioner's Office;
- To appoint a Data Protection Officer;
- To ensure transparency (Privacy Notices); and
- To ensure that data subjects can exercise their DPA 2018 rights

5.8. If this Agreement is entered into after the parties have begun sharing Data with each other, it shall apply retrospectively to the processing of such Data from the date on which such sharing began.

5.9. All Parties shall, through the submission of an annual NHS Data Security and Protection Toolkit, put in place appropriate technical and organisational measures to ensure the protection of Personal Data subject to this Agreement against the accidental loss or destruction of or damage to Patient 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 by the relevant 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.

5.10. All Parties shall only process patient Information as is necessary to perform its obligations under this Agreement and only in accordance with the instructions set out in this Agreement and, in particular shall not use or process patient Information for any purpose other than those stated.

5.11. All Parties must comply with subject access and data subjects rights related to the Personal data they hold. Where these are received by any of the Parties, they will be forwarded promptly to the relevant Party for action.

5.12. All Parties must assist each other in meeting their GDPR obligations in relation to the security of processing, the notification of Personal data breaches and data protection impact assessments.

5.13. Any minor changes to this Agreement that may become necessary from time to time shall be explicitly agreed by the Joint Controllers, as a written variation.

5.14. In the event of major changes being required, the Parties shall terminate this Agreement and replace it in full with an updated version. Such termination and replacement may also be initiated by any Party.

5.15. Parties can choose to use the **Information Sharing Gateway ("ISG")** as the online medium and depository where this Agreement and subsequent variations may be reviewed and approved as applicable.

5.16. Agreed Sharing Mechanisms: This is the technical means by which parties shall transmit personal data between each other. It could be one or more of these listed below.

- **EMIS Health Systems Local Record Sharing – Integrated Care:** This shall be used to transmit patients' medical records between partners to this agreement. The system will enable each EMIS Partner share a patient's medical record held on secure EMIS Web clinical system in order to provide end of life palliative care services within the West Kent area.

  The information is accessed in real time and on-demand, meaning that data from the source GP record is neither extracted, nor uploaded, nor sent anywhere in real time and on-demand.

- **Vision 360:** Vision 360 Practice Access provides secure, remote access to a patient's clinical data including medical history, therapy and test results. It allows Vision and EMIS Web Practices you to share, view, record and edit patient consultation details between the two systems irrespective of technological and organisation boundaries.

- **MIG:** Healthcare Gateway is the system supplier of Medical Interoperability Gateway (MIG) system that provides healthcare professionals with instant access to real-time information about a patient in order to make informed treatment decisions faster, and improve the efficiency of care by preventing unnecessary hospital admissions/appointments and duplicated tests.

  The MIG is a secure middleware technology which will enable the two-way exchange of patient information between the Registered Partners.

6.0 Description of Personal Data

6.1. The Patient Information covered in this Agreement is as detailed in section 6.3 and where relevant is indicated as Special categories of personal data.

6.2. Parties to this Agreement acknowledge that disclosure of Personal data as may contain Patient Information must be under the responsibility of a registered health or social care professional.

6.3. The Patient Information covered in this Agreement is as detailed below:

• Patient name • Patient address • NHS Number	• Medication including Current, Past and Issues
• Patient e-mail	• Risks and Warnings
• Patient phone number	• Procedures
• Summary, including Current Problems,	• Investigation

Current Medication, Allergies, and Recent Tests	• Examination (e.g. Blood Pressure) • Events consisting of Encounters, Admissions and Referrals
• Problem view	• Care and Support Plan including free text
• Diagnosis View	• Treatment Escalation Plans
• Contact details for carers/legal guardians	• Other related medical information

7.0 Data Protection Legislations

7.1. All Parties shall comply with all aspects of the GDPR, DPA2018, Human Rights Act 1998 and Common Law Duty of Confidentiality in relation to the processing of Personal data and Special categories of personal data as part of this Agreement.

7.2 Each party is required to keep and maintain a record of processing activities (also known as the 'data flow map') in accordance with the Data Protection Legislation. The record shall contain all of the following information:

- the name and contact details of the Controller and "Joint Controllers", the Controller's representative and the Data Protection Officer;
- the purposes of this Processing;
- a description of the categories of Data Subjects and of the categories of Personal Confidential Data;
- the categories of recipients to whom data has been, or will be, disclosed; and
- where applicable, any transfers of data to a third country and the appropriate safeguards relied upon to do so.

7.3. All Parties shall only process Personal data in accordance with this Agreement, unless empowered to do so by a legal obligation, in which case they shall inform the other Parties of this obligation.

7.4. All Parties shall put in place appropriate technical and organisational measures against any unlawful and unauthorised processing of Patient Information and against accidental loss, destruction of and damage to Patient Information.

7.5 No Party shall cause or allow Patient Information to be transferred to any territory or stored outside the United Kingdom without the prior written permission of all the other Parties.

7.6 **Indemnities and Warranties:** Each party undertakes to indemnity other parties to allow for recovery of costs by an 'innocent' party from a culpable one, if a claim is brought or regulatory action is taken due to a fault of the culpable party. For instance, where a data breach occurs, the breaching Party shall indemnify the relevant Party against and compensate for any loss (financial or otherwise) that the relevant Party sustains due to any failure by the breaching Party or employees or sub-contractors to act in accordance with the terms of this Agreement and relevant legislation.

8.0 The legal basis for sharing patient confidential data

8.1. Personal/Special categories of personal data must be processed 'fairly' and 'lawfully'. The lawful basis of Joint Control is set out in the GDPR / DPA2018.

8.2. Legal duties, robust public interests and vital interests are related to conditions in the GDPR / DPA 2018. In addition, sharing must be 'fair' by ensuring the data subject is aware, by way of access to a Privacy Notice, of what is being shared and for what purpose. Only in situations where informing the data subject is likely to cause them or another significant harm/distress, or prejudice actions or outcomes of a situation, can this principle be set aside.

8.3. The legal basis for processing Personal data specified above, under the GDPR, is as follows:

- Lawfulness of processing- Article 6 (1)(e) '…for the performance of a public task carried out in the public interest or in the exercise of official authority.
- Processing of Special categories of personal data Article 9 (2)(h) '…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems'.
- Sharing Personal Data is carried out subject to the conditions and safeguards of Obligation of Professional Secrecy Article 9 (3).
- Sharing is done in accordance with DPA 2018 S.11 (1) by:
- By or under the responsibility of a health professional or a social work professional, or
- By another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

8.4. In addition:

- **The National Data Guardian Report 2016**
  In accordance to clause 3.2.10 (page 25-26), the National Data Guardian Report 2016 recommended to the Secretary of State (SOS) for Health and Social Care that "risk stratification **for case finding and/or targeting purposes",** where carried out by a healthcare provider (acting as a Data Controller) involved in an individual's care or, by **a Processor acting under contract with such a provider, should be treated as 'Direct Care'** for the purpose of opt-out (and therefore should not be subject to the opt-out of Personal Confidential Data being used for purposes beyond direct care).
- Health and Social Care (Safety and Quality Act) 2015
  S3 of the HSCSQA inserts a statutory 'duty to share' into the Health and Social Care Act 2012 (s251B) information if it is likely to facilitate the provision to the patient of health services or adult social care in England and it is in the patient's best interests.
- The Common Law Duty of Confidentiality
  Where Personal data has been confided, or where information is clearly confidential in nature, it shall only be used for the purpose for which it was given and not be disclosed for any other purpose without permission.
- Article 8 of the European Convention of Human Rights
  Sharing under this Agreement shall not interfere with data subjects' enjoyment of their Article 8 rights except such as is in accordance with the law or other compatible exceptions.

9.0 Appointment of a Processor

9.1 The Parties to this Agreement are the Controllers of Personal Confidential Data disclosed through the EMIS or any other relevant clinical system, and they shall "jointly" determine the purposes and means of processing carried out by any processor, if appointed.

9.2 Where applicable, such jointly appointed Data Processor would owe its obligations as a Processor to all parties to this Data Sharing Agreement.

10.0 Policies and Procedures

10.1. All Parties shall have appropriate policies covering confidentiality, information security, data protection and records management. This also includes policies to cover the identification and management of serious incidents and data breaches which all staff should be made aware of and adhere to.

10.2 These will describe individual responsibilities for the handling of Personal data, communicating to patients their individual rights including the right to object and these will be rigorously applied.

10.3. All Parties shall provide copies of the policies referred to above on request.

11.0 Viewing Records

11.1. All Parties will be able to view applicable patients' records contained within EMIS clinical system for the duration of Hospice in the Weald Hospice providing end of life palliative care to patients in West Kent, and will be required to follow the standards below:

- The sharing of Personal data between Parties is underpinned by this data sharing agreement, of which a copy is sent to EMIS (if required) who then technically enables an internal data sharing agreement within the EMIS clinical system, which each Party has to independently authorise, before Personal data sharing can take place.

11.2. Any Personal data shared between the Parties to this Agreement for the purposes so stated in, must not be disclosed to any other third party. In addition:

- Each Party shall ensure that access to information under this Agreement will only be granted to those staff who 'need to know' the information and with the requisite data protection training.
- The Parties shall comply with the requirements of GDPR and DPA 2018 in handling the shared Personal data securely including having a process in place that inform patients about their individual rights.
- Confidential information should be sent by NHS email to NHS email or to another encrypted email address where appropriate.

11.3. These conditions ensure that only those (staff) with valid credentials and reasons are given access to view a Personal data and that they only access/view necessary parts of a patient's data. With regards to the EMIS clinical system this provides an audit trail of all access to records. All Parties must ensure that all staff with access to the EMIS clinical system have been fully trained on the system, and understand that access to a patient's record is audited.

12.0 Security: General

12.1. No Party will be part of this Agreement unless able and willing to comply with the terms of this Agreement and any Party reserves the right to terminate this Agreement if any other Party is unable to agree necessary amendments in future.

12.2. No Party shall, under any circumstances, share, disclose or otherwise reveal Patient Information (in whole or in part) to any individual, business or other organisation not directly involved in delivery of the ongoing care of the patient without the explicit written consent of the other Parties or without another legal basis which overrides this requirement.

12.3. All Parties shall be immediately notified by the Party experiencing any untoward incidents or activities that suggest non-compliance with any of the terms of this Agreement. This includes 'near-miss' situations; damage to or loss of Personal data; or inappropriate disclosure of Patient Information results.

13.0 Security: Physical

13.1. All Parties shall ensure that all Patient Information is physically protected from accidental or deliberate loss or destruction arising from environmental hazards such as fire or flood.

13.2. All Parties shall ensure that all Patient Information is accessed on premises, or systems that are adequately protected from unauthorised entry and/or theft of Patient 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.

14.0 Security: IT Systems

14.1. Patient Information must under no circumstances be stored on unencrypted portable media or devices such as laptops or USB memory sticks or CD-ROM unless agreed in writing.

All Parties shall ensure that:

- All portable media used for storage or transit of Patient Information are fully encrypted in accordance with NHS Guidelines on encryption to protect Personal data (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.

14.2. No Party shall allow its employees to hold Patient Information on their own personal computers/electronics devices.

14.3. All Parties shall ensure adequate back-up facilities to minimise the risk of loss of or damage to Patient Information and that a robust business continuity plan is in place in the event of restriction of service for any reason.

14.4. No Party shall transmit Patient Information except by email or as an attachment encrypted to 256 bit AES\Blowfish standards or from NHS mail to NHS mail, or between secure email services as approved by HM government or NHS Digital.

14.5. All Parties shall only make printed paper copies of Patient Information if this is essential for delivery of the service.

14.6. All Parties shall store printed paper copies of Patient Information in locked cabinets when not in use and shall not remove from the premises unless this is essential for delivery of the service.

14.7. All Parties shall provide the other Parties, upon request, with confirmation that they are compliant with the Data Security and Protection Toolkit (DSPT) before the other Parties can allow any access to networked IT systems (e.g. N3, Summary Care Record, etc.) if relevant.

15.0 Data Retention and Secure Destruction

15.1. NHS data are subject to legal retention periods and should not be destroyed unless in accordance with the Records Management Codes of Practice for Health and Social Care 2016. Therefore, each Party shall ensure it has a written policy and procedure for the archiving, retention and disposal of information.

15.2 Where personal data has been identified for disposal:

- All Parties shall ensure that Patient Information held in paper form (regardless of whether as originally provided by another Party or printed from their IT systems) is destroyed using a cross cut shredder or subcontracted to a confidential waste company that complies with European Standard EN15713.

- All Parties shall ensure that electronic storage media used to hold or process Patient Information is destroyed or overwritten to current CESG standards as defined at www.cesg.gov.uk

- In the event of any bad or unusable sectors that cannot be overwritten, the relevant Party shall ensure complete and irretrievable destruction of the media itself.

- All Parties shall provide the other Parties with copies of all relevant overwriting verification reports and/or certificates of secure destruction of Patient Information at the conclusion of this Agreement.

15.3 Notwithstanding the above, by default any Processor if appointed by the Parties under the terms of this Agreement will de-identify or delete any data received from the Controller(s) within a maximum of two years from the date of the last data being received from the Controller(s). And the Processor undertakes not to transfer any patients' personal data to its own database or server; except completely anonymised data.

16.0 Monitoring & Audit

16.1. All Parties shall permit the other Parties to monitor compliance with the terms of this Agreement, by:

- Allowing their employees or nominated representatives to enter any premises where Patient Information is held, at reasonable times and with or without prior notice, for the purpose of inspection in relation to this Agreement.
- Provide independent assurance of the self-audited Information Governance/Data Security and Protection Toolkit performance measures where the other Parties are required to comply.

16.2. An audit trail of any user, who viewed Personal data for a patient, as held on any party's system.

17.0 Freedom of Information

17.1. All Parties acknowledge and agree to the requirements of the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR), where applicable, with regards to this Agreement; including updating their FOI publication scheme with the purpose of this Agreement.

17.2. At least the basic details of this Agreement would be disclosed, if requested, under the requirements of the FOIA.

17.3. All Parties shall consult the other Parties to this Agreement regarding commercial or other confidentiality issues in relation to this Agreement, however the final decision about disclosure of information or application of exemptions shall rest solely with the relevant Controller.

18.0 Legislation, Codes of Practice and Guidance

18.1. The following provide gateways and guidance for signatory partners to share information and must be complied with where relevant:

- Common Law (Duty of Confidence);
- General Data Protection Regulation
- Data Protection Act 2018
- Human Rights Act 1998 (Article 8)
- Freedom of Information Act 2000
- NHS and Community Care Act 1990
- Health Act 1999 (Section 31)

- NHS Act 2006 (Section 82)
- Health and Social Care Act 2012
- Medical Act 1983 and the Medical Act Amendment Order 2000
- Mental Health Acts 1983 and 2007
- Mental Capacity Act 2005
- Regulation of Investigatory Powers Act 2000
- Confidentiality: NHS Code of Practice (November 2003)
- Confidentiality: NHS Code of Practice Supplementary Guidance on Public Interest Disclosures (November 2010)
- Health and Social Care (Safety and Quality) Act 2015
- HSCIC Guide to Confidentiality
- Information Governance/Caldicott 2 Review: To Share or Not to Share
- Records Management NHS Code of Practice 2016
- NHS England Safe Haven Procedure
- NHS Constitution
- Information Security Management Code of Practice
- Data Sharing Code of Practice
- Privacy Notices Code of Practice
- Kent and Medway Information Sharing Agreement
- Any other relevant legislation, standards or guidance

18.2. The Parties acknowledge and agree that they will share information whenever one or all Parties are under a statutory duty to do so. In this case, the Party requesting the information shall make clear in its request to share, the legislation underpinning the request for Personal data and the disclosure of Personal data shall comply with the relevant legislation and be made in accordance with the terms of this Agreement, if applicable.

19.0 Accession of a new party/Voluntary Exit/Expulsion

19.1 **Accession of a new party:** Any person who is not one of the original Parties to this Agreement but who subsequently wishes to join (this Data Sharing Agreement) shall become a Party to this Agreement once they have executed an 'Agreement of Accession'. Consequently, the New Party shall effectively be a party to this Joint Controller's Data Sharing Agreement from and including the date of their accession to the Agreement or the date the New Party starts to be a disclosing party/receiving party in relation to shared personal data under the terms of this Agreement.

19.1.1 Existing Parties will be notified of the accession of the new party within 10 working days, with the opportunity to express their reservations, if any during this time.

19.1.2 The execution of the Agreement of Accession may be executed via the document at appendix 1 and/or via electronic means such as on the ISG.

19.2 **Voluntary Exit:** A party to this Agreement can give notice to leave on its own accord, so long as it informs the other parties with at lWest 2 calendar months' notice. Any Party who is a Current Party to this Agreement and whose voluntary exit from has been approved accordingly, shall cease to be a Party to this Agreement accordingly.

19.3 **Expulsion**: Any Current Party to this Agreement who is found to be in breach of the term(s) of this Agreement may be expelled; and when this occurs shall cease to be a Party to this Agreement accordingly.

19.4 **Consequences of Termination**: Prior to the Actual Leaving Date (in the case of each Voluntary Exit Party), and prior to or (at the latest) on the Expulsion Date (in the case of each Expelled Party), the Remaining Parties and the relevant Exiting Party shall determine a detailed plan of prerequisites and actions or omissions that must be effected by the Remaining Parties and such Exiting Party. Such plan shall, amongst other matters, address as applicable:

- the communication of such changes to Data Subjects;
- the amendment or replacement of the Patient Privacy Notices and the Staff Privacy Notices of each Party and the publication of the amended or replaced notices to Data Subjects;
- the cessation of (a) the relevant Exiting Party's disclosure in its capacity as a Disclosing Party and its Shared Data Processors of its Shared Personal Data under this Agreement, and (b) the cessation of the access to and Processing of such Shared Personal Data, in its capacity as a Receiving Party, by each of the Remaining Parties (including their permitted Staff) and their Processors;
- the removal of the interfaces and other means by which the relevant Exiting Party's Electronic Information Processing Systems are connected with the Remaining Parties' Electronic Information Processing Systems (and each of them); and
- the timescales within which such actions or omissions will be effected

20.0 Review and Termination

20.1 This Agreement shall be reviewed at lWest every 12 months especially for reconsideration of the sharing mechanism to another model, to check if the expected clinical benefits have materialised and to review IG risks.

20.2 Additionally, this Agreement would be reviewed (and terminated/replaced) subject to any change in applicable legislations, change in business needs or end of a relevant service provision by any of the parties to this Agreement.

21.0 Close down Procedure

21.1 This close-down procedure to be followed in the event of the termination of this Agreement is that in such an event, all activities and projects initiated under this Agreement shall terminate in a controlled manner.

22.0 Relevant Publications

22.1. For NHS organisations a range of publications can be obtained from www.dh.gov.uk, www.nhsemployers.org and www.connectingforhealth.nhs.uk, including relevant NHS codes of practice and standards. These cover areas including confidentiality, information security management, employment check standards and records management. Non-NHS organisations should likewise have robust policies and procedures in place to meet the requirements of the Data Security and Protection Toolkit. It is the responsibility of all Parties to ensure they are compliant with these practices and standards.

23.0 Legal Jurisdiction

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

23.2. In the event of a dispute, the parties to this Agreement agree to attempt to resolve such issues according to NHS dispute resolution procedures.

Appendices

Appendix 1: List of Practices

Appendix 2: New Party Agreement of Accession (*Generic*)

Requisites and Validation

The purpose of this Agreement:

This Agreement provides for openness and transparency in Personal data sharing, as well as appropriate governance and support, in order to assist signatory organisations to share Personal data lawfully, safely and securely.

Provisos:

- Signatory partners recognise that the sharing of Personal data must be justified on the merits of each case;
- All signatory partners will be informed of any future Health or Social care organisations (or GP Practices) wishing to join this Agreement; and
- All signatory partners are required to review and approve this Data Sharing Agreement at start and periodically as agreed.
- This Agreement can also be reviewed where there is a significant change in applicable legislations or relevant NHS policy.
- Data Protection Contact
  Each Party shall nominate a Data Protection Contact (ideally IG Lead/DPO) who will be the point of contact for the management of this Agreement.

  Each Party shall ensure that any data protection matters relating to this Agreement in respect of the dispute about data sharing/Processing relating directly to this Agreement are directed promptly to the nominated Point(s) of Contact of the relevant Party.

Organisation:	Hospice in the Weald

SIRO or Caldicott Guardian signature:	
Print title:	**Medical Director and Caldicott Guradian**
Print name:	**Dr Helen McGee**
Date:	**26.11.20**

(Print name & position of authorised signatory e.g. Caldicott Guardian, SIRO, Chief Executive, Director)

Organisation:	Name of the Practice

SIRO or Caldicott Guardian signature:	
Print title:	
Print name:	
Date:	

(Print name & position of authorised signatory e.g. Caldicott Guardian, SIRO, Chief Executive, Director)

Counterparts

This agreement may be signed in any number of separate counterparts, each of which when signed and dated shall be an original, and as such counterparts taken together shall constitute one and the same agreements.

Alternatively, this Agreement can be agreed and executed by electronic means such as but not limited to the Information Sharing Gateway ("ISG").

West Kent Practices	
West Kent Area	**Tunbridge Wells Area**
CRANE SURGERY	ABBEY COURT MEDICAL CENTRE
HOWELL SURGERY (Brenchley & Horsmonden)	CLANRICARDE
Ivy Court	GROSVENOR MEDICAL CENTRE
LAMBERHURST SURGERY	KINGSWOOD SURGERY
MARDEN MEDICAL CENTRE	LONSDALE MEDICAL CENTRE
NORTH RIDGE SURGERY	RUSTHALL MEDICAL CENTRE
OLD PARSONAGE SURGERY, GOUDHURST	ST ANDREWS MEDICAL CENTRE
Old School Surgery	ST JAMES MEDICAL CENTRE (Grosvenor)
ORCHARD END SURGERY	SPELDHURST AND GREGGSWOOD - THE OLD BAKERY
STAPLEHURST MC (Malling Health Four)	WATERFIELD HOUSE SURGERY
WISH VALLEY SURGERY	
YALDING SURGERY	**Tonbridge Area**
Sevenoaks Area	HILDENBOROUGH MEDICAL GROUP (Trenchwood)
AMHERST MEDICAL PRACTICE	TONBRIDGE MEDICAL CENTRE
BOROUGH GREEN MEDICAL CENTRE	WARDERS MEDICAL CENTRE
EDENBRIDGE MEDICAL PRACTICE	WOODLANDS HEALTH CENTRE
WINTERTON SURGERY / WESTERHAM	HADLOW MEDICAL CENTRE
OTFORD MEDICAL PRACTICE	
SOUTH PARK MEDICAL CENTRE	
ST JOHNS MEDICAL PRACTICE	
TOWN MEDICAL CENTRE	

THIS Agreement is dated [DATE]

PARTIES

(1) [FULL PARTY NAME] [*Guidance Note: party to be defined*];

(2) [FULL PARTY NAME] [*Guidance Note: party to be defined*];

(3) [FULL PARTY NAME] [*Guidance Note: party to be defined*];

(4) [FULL PARTY NAME] [*Guidance Note: party to be defined*],

(Together, the "**Current Parties**"); and

[FULL NAME OF NEW PARTY] ("**New Party**") [*Guidance Note: party to be defined*].

BACKGROUND

(A) The Data Sharing Agreement was entered into between [insert a list of the original Parties] on [DATE].

(B) Under clause 10.1 (*Accession of New Party*) of the Data Sharing Agreement, a person may become a Party to that agreement subject to the terms of that clause.

(C) It is proposed that the New Party becomes a party to the Data Sharing Agreement.

1 Definitions and Interpretation

1.1 The following definitions and rules of interpretation apply in this Deed:

"**Data Sharing Agreement**" means the Agreement that was entered into on [DATE] between the stated parties as above.

1.2 The definitions set out the Data Sharing Agreement are incorporated into this Agreement.

2 New Party's accession

With the consent of the Current Parties, the New Party shall be joined as a party to the Data Sharing Agreement with effect from the date of this Agreement. The New Party's participation shall be subject to the terms set out in this Agreement.

3 New Party's obligations

The New Party agrees that it shall be bound by the terms of the Data Sharing Agreement as a Party to the Agreement.

4 General

This Agreement may be executed in one or more counterparts. Any single counterpart or a set of counterparts executed, in either case, by the Parties shall constitute a full original of this Agreement for all purposes.

Each party to this Agreement submits to the non-exclusive jurisdiction of the English courts and agrees that this Agreement is to be governed and construed according to English law.

In witness of whom the parties to this Agreement have executed it as a Deed and delivered it on the date stated at the beginning of it.

New Party	
Name:	
Position:	
Signature:	
Date:	

(Print name & position of authorised signatory e.g. Caldicott Guardian, SIRO, Chief Executive, Director)

Representative of Current Parties	
Name:	Julian Le Saux
Position:	Practice Manager
Organisation:	The Crane Surgery, Rectory Fields, Cranbrook, Kent TN17 3JB
Signature:	Julian Le Saux
Date:	2/1/21

(Print name & position of Authorised signatory e.g. Caldicott Guardian, SIRO, Chief Executive, Director)

*[**Guidance Note:** one of the current parties can be the nominated representative for the current parties especially where it is a large group]*

Witnessed By:

Name:	
Position:	
Signature:	
Date:	

[Guidance Note:** Intended to be executed by relevant parties as a Deed.**]