

# Health and care: Data sharing and processing agreement (DSPA)

## Table of Contents

### DATA SHARING AND PROCESSING AGREEMENT

#### Part 1

1. Set out what this Agreement will cover.
2. Summary of how data will be used and shared.
3. Data Protection Impact Assessment (DPIA)
4. Confirm the level of identifiability of the data for each party.
  - a. If using pseudonymised data, provide further details.
  - b. If using anonymised data, provide further details.
5. What are the purposes for using or sharing the data?
6. What are the benefits of using or sharing the data?
7. For this agreement, which types of personal data do the Parties need to use and why?
8. Which types of sensitive (including special category) data do the Parties need to use or share?
9. Who are the individuals that can be identified from the data?
10. Describe the flows of data.
11. Under Article 6 of UK General Data Protection Regulation (UK GDPR), what is the lawful basis for processing personal data?
12. Under Article 9 of UK General Data Protection Regulation (UK GDPR), what is the lawful basis for processing special category data?
13. What is the legal basis for sharing or using health and care data under the common law duty of confidentiality?
14. How will the Parties ensure that information is safe and secure?
15. For this Agreement, how long are the Parties planning to use the data for?
16. For this Agreement, how long do the Parties intend to keep the data?
17. What will happen to the data at the end of this Agreement?
18. How will the Parties comply with the following data subject rights (where they apply)?
  
19. Will the national data opt-out need to be applied? Which organisation is responsible for managing this process?
20. List the organisation(s) that will decide why and how the data is being used and shared (Controllers).
21. List the organisation(s) that are being instructed to use or share the data (Processors).
22. List any organisations that have been subcontracted by your Processor to handle data (Sub-Processors).
23. How will the Parties ensure data accuracy and that updates to the data are communicated where necessary?

24. Describe how data breaches will be managed.
25. Set out any terms agreed by the Parties regarding liability.
26. If applicable, provide details of any agreed variation of terms from Part 2 of this agreement.
28. Detail any processing that has not been captured above.
29. Set out the review period for this agreement.
30. Reviewers
31. Signatories

Part 1 Annex 1 – List of Controllers and Processors and their named points of contact

Part 2

1. BACKGROUND AND SCOPE
2. DEFINITIONS AND INTERPRETATION
3. DURATION AND CONSIDERATION
4. GENERAL OBLIGATIONS
5. CONTROLLER OBLIGATIONS
6. ADDITIONAL ALL PARTY AND PROCESSOR SPECIFIC OBLIGATIONS Bookmark missing
7. PERSONAL DATA BREACHES
8. DATA SECURITY ARRANGEMENTS
9. LIABILITY
10. VARIATION OF AGREEMENT
11. FREEDOM OF INFORMATION AND ENVIRONMENTAL INFORMATION REGULATIONS
12. GENERAL
13. TRANSPARENCY
14. DISPUTE RESOLUTION
15. TERMINATION

## **DATA SHARING AND PROCESSING AGREEMENT**

Issued under UK General Data Protection Regulation (UK GDPR) and Data Protection Act  
2018

### **BETWEEN**

**The Controller(s) and Processor(s) (where applicable),**

**as set out below**

(Collectively the 'Parties'.)

Controller: **DUNCHURCH SURGERY**

Processor: **Primary Care IT Ltd**

### **In support of**

The Processing (including sharing) of personal data in the operation of services within the  
health and care system as set out in in Part 1.

# Part 1

## Scope of agreement

This Agreement sets out the details relating to inter Party Data Processing Activities to which the Parties have agreed.

The Definitions in Part 2 of the Agreement shall also apply to this Part 1.

In the event of any inconsistency between Part 1 and Part 2 of this Agreement, the provisions of this Part 1 shall prevail.

### 1. Set out what this Agreement will cover.

<input type="checkbox"/>	Controller to Controller data sharing
<input type="checkbox"/>	Joint Controller arrangement
<input checked="" type="checkbox"/>	Controller to Processor instruction

### 2. Summary of how data will be used and shared.

The PCIT toolset (templates, protocols and searches) has been procured to support the practice with contractual, compliance, and patient care objectives efficiently within the EHR system.

Practices should be better able to meet QOF/IIF targets alongside maximising current national and local contracts.

The tools will benefit patients by utilising “pop ups” to alert practice staff to several indicators without the need of a consultation i.e. bloods and/or medication review needed. For example when a patient calls the practice, the pop up will notify of applicable bloods/vaccines/screenings to offer the patient. During use of the PCIT toolset no data is shared with the PCIT team and remains entirely within practice foundation electronic health records. Data will be looked at when PCIT support teams are assisting practice team members with queries or issues with the PCIT tools.

### 3. Data Protection Impact Assessment (DPIA)

The LMC & ICB have confirmed the following to ensure that roll out of the PCIT toolset can continue.

We (the ICB, LMC and PCIT) are currently developing a robust DPIA that allows PCIT to provide a reactive service whilst ensuring appropriate information governance. It is going to take some time to fully understand the data privacy implications, and required mitigations to ensure patients identifiable data and practices are GDPR compliant. However, in the interim, we understand it is unhelpful for patients to miss out on care and/or practices miss enhanced service targets. As such we have worked together and agreed:

1. Practices will give PCIT EMIS logins with RBAC codes B1700 and B0994
2. These codes will allow templates and searches to be imported and run on your system and enable alerts. However, these codes do NOT allow any patient data sharing, so a DPIA is NOT required at this time.
3. If your practice subsequently had any issues with the new system that requires PCIT to potentially see patient identifiable data, you will need to:
  1. have the PCIT employee sign a confidentiality agreement,
  2. 'screen share' whilst investigating and resolving the issue,
  3. provide an individual to be available to 'click' between screens whilst the PCIT employee fixes the issue.

We appreciate that the proposed solution could be labour intensive for practices, so practices may wish to ignore any PCIT 'teething problems' until the DPIA is agreed. Arden's searches will not disappear on 28 February and are unlikely to change before QOF/IIF year end, so practices could continue to rely on these.

If you have any concerns or would like to discuss this further, please contact Warwickshire LMC at [warwick.lmc@nhs.net](mailto:warwick.lmc@nhs.net)

#### **4. Confirm the level of identifiability of the data for each party.**

The practice retains identifiable patient data within the clinical system under strict governance for direct care purposes. The PCIT searches will help them to create reports that may be shared with other parties as they wish but this would be covered under a separate data sharing agreement with the relevant parties.

When PCIT support practice team members their helpdesk, the PCIT team will need to review electronic health records of the relevant patients that the query relates to. This will be done by the practice sharing their screen with PCIT support desk so that the investigation can take place whilst the practice is on the call. This could include patient names, addresses, telephone numbers and details of their health records. This data is viewed on screen by PCIT team members and there is no transfer of data.

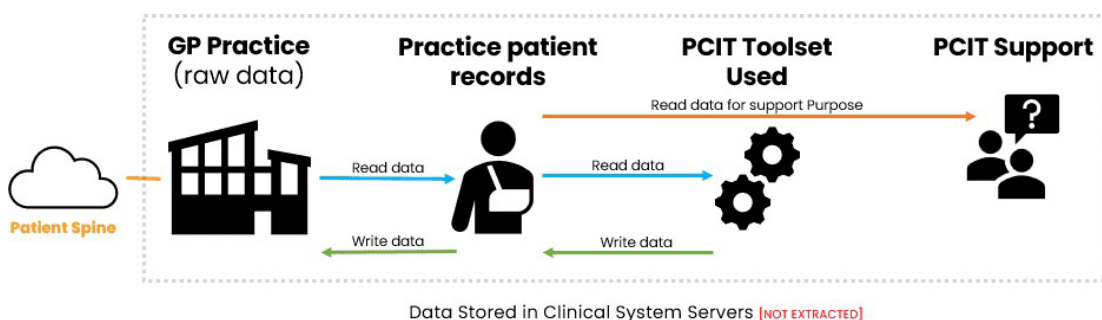
### Data Processing General Products

Primary Care IT supports practices with decision support tools, contract management tools, as well as any other resources practices may need for the efficient running of their practice.

The products provided depend on the subscription or individual products purchased.

#### Products covered via this data processing:

- PCIT Toolset
- One Recall
- GP Contract Pro
- PCN DES
- CQC Navigator
- One Results
- One Monitoring
- Referral Tree
- PTP
- Localisation



## 5. What are the purposes for using or sharing the data?

The purpose of the data controller collecting information is to provide medical services, provide data to commissioners. By bringing in the PCIT Toolkit within the EHR we will do this more effectively and efficiently.

Data processed remains entirely within the practice's native Electronic Health Record (EHR) system. The use of PCIT toolset it allows practices to do this quicker, easier and with more efficiently.

This includes searches that practices can run and view, examples of which are below:

- Diagnostic information.
- Treatment records.
- Risk assessments.
- Contract management
- Monitoring and recalls.

All of which will assist practices with contractual, compliance, and patient care objectives efficiently within the EHR system.

When support teams are assisting practice members this is to help them understand why a patient is not achieving a key performance indicator, where there appears to be a problem or the practice can't understand why the patient is showing as not having or having an element of care.

## 6. What are the benefits of using or sharing the data?

The Practice will benefit from the support of the PCIT team in troubleshooting issues with data in their practice. The level of expertise that the practice has access to will be well in excess of that which they would be able to call upon without this resource.

The tools will benefit patients by utilising "pop ups" to alert practice staff to several indicators without the need of a consultation i.e. bloods and/or medication review needed. For example when a patient calls the practice, the pop up will notify of applicable bloods/vaccines/screenings to offer the patient.

The PCIT toolsets (made up of searches, templates and protocols) are used to assist practices in:

- Managing national contracts and ensuring regulatory compliance (e.g., CQC, MHRA, CAS, and NPSA alerts).
- Streamlining operational workflows within their EHR system.
- Optimizing patient care through efficient data handling and reporting.
- Practices should be better able to meet QOF/IIF targets
- Pop ups within EHR to assist patient care

The existing system can do all of the above things but with the use of PCIT toolset it allows practices to do this quicker, easier and with more efficiently.

This can be measured in time saved, increase in QOF/IIF target, improved coding accuracy, income generation and patient satisfaction scores.

The PCIT toolset supports practices in processing their own data for example it simplifies QOF coding to increase consistency of input and therefore the integrity of the data is better. This takes place securely within the native EHR environment. No data is transferred to PCIT or external systems, see above.

**7. For this agreement, which types of personal data do the Parties need to use and why?**

<input checked="" type="checkbox"/>	Forename	<input checked="" type="checkbox"/>	Physical description, for example height	<input type="checkbox"/>	Photograph / picture of people
<input checked="" type="checkbox"/>	Surname	<input checked="" type="checkbox"/>	Phone number	<input type="checkbox"/>	Location data e.g. · IP address · Other
<input checked="" type="checkbox"/>	Address	<input checked="" type="checkbox"/>	Email address	<input type="checkbox"/>	Audio recordings
<input checked="" type="checkbox"/>	Postcode full	<input checked="" type="checkbox"/>	GP details	<input type="checkbox"/>	Video recordings
<input type="checkbox"/>	Postcode partial	<input type="checkbox"/>	Legal representative name (personal representative)	<input type="checkbox"/>	Other
<input checked="" type="checkbox"/>	Date of birth	<input checked="" type="checkbox"/>	NHS number	<input type="checkbox"/>	None
<input checked="" type="checkbox"/>	Age	<input type="checkbox"/>	National insurance number		
<input checked="" type="checkbox"/>	Gender	<input checked="" type="checkbox"/>	Other numerical identifier EMIS number		

PCIT does not require access to specific identifying details such as names, addresses, or contact information. However, the team needs to access all coded data within patient records related to the issues under investigation. Due to the nature of these issues, this may include a broad range of data such as:

- Medical conditions (e.g., diabetes, asthma).
- Measurements (e.g., weight, height).
- Test results (e.g., HbA1c blood tests).

This information is essential to accurately identify and resolve issues affecting practice performance.



**8. Which types of sensitive (including special category) data do the Parties need to use or share?**

Type of data	Reason why this is needed (leave blank if not applicable)
<input checked="" type="checkbox"/> Information relating to an individual's physical or mental health or condition, for example information from health and care records	<p>PCIT could need to access <b>special category data</b> relating to an individual's physical or mental health or condition, as recorded in health and care records. This includes coded information about medical conditions, treatments, and results (e.g., diabetes, asthma, HbA1c results) that directly impact KPI performance.</p> <p>This data is essential for identifying and resolving issues within patient records that are preventing practices from meeting KPI requirements. Without this level of detail, it would not be possible to provide accurate support or ensure compliance with contractual obligations, which ultimately impacts patient outcomes and practice performance.</p> <p>This information would only be accessed in conjunction with a practice member who has reported an issue for investigation via a screen share with PCIT.</p>
<input type="checkbox"/> Biometric information in order to uniquely identify an individual, for example facial recognition	
<input type="checkbox"/> Genetic data, for example details about a DNA sample taken as part of a genetic clinical service	
<input type="checkbox"/> Information relating to an individual's sexual life or sexual orientation	
<input checked="" type="checkbox"/> Racial or ethnic origin	<p>This data is essential for supporting issues focused on particular groups, such as vaccination campaigns or care processes targeting patients from BAME backgrounds. For</p>

		example, it may be used to identify and review patients with a high BMI who require targeted interventions or monitoring.
<input type="checkbox"/>	Political opinions	
<input type="checkbox"/>	Religious or philosophical beliefs	
<input type="checkbox"/>	Trade union membership	
<input type="checkbox"/>	Information relating to criminal or suspected criminal offences	
<input type="checkbox"/>	None of the above	

**9. Who are the individuals that can be identified from the data?**

<input checked="" type="checkbox"/>	Patients or service users
<input checked="" type="checkbox"/>	Carers
<input checked="" type="checkbox"/>	Staff
<input checked="" type="checkbox"/>	Wider workforce
<input type="checkbox"/>	Visitors
<input type="checkbox"/>	Members of the public
<input type="checkbox"/>	Other

**10. Describe the flows of data.**

Data flow name	Going from	Going to	Data description
Support session data	GP system	PCIT team	Coded patient data and system configuration details accessed for issue resolution.  This information would only be accessed in

			conjunction with a practice member who has reported an issue for investigation via a screen share with PCIT.
--	--	--	--

**11. Under Article 6 of UK General Data Protection Regulation (UK GDPR), what is the lawful basis for processing personal data?**

The (DUNCHURCH SURGERY) lawful basis for processing personal data is **to perform a public task.**

Primary Care IT Ltd **have a contractual obligation with the (DUNCHURCH SURGERY)**

**12. Under Article 9 of UK General Data Protection Regulation (UK GDPR), what is the lawful basis for processing special category data?**

The (DUNCHURCH SURGERY) lawful basis for processing special category data is for the practice to comply with the legal obligations to provide or manage health or social care services and for public health.

<input type="checkbox"/>	(b) We need it to comply with our legal obligations for employment
<input type="checkbox"/>	(f) We need it for legal claims, to seek legal advice or judicial acts
<input type="checkbox"/>	(g) We need to comply with our legal obligations to provide information where there is a <a href="#">substantial public interest</a> , as set out in <a href="#">this list</a>
<input checked="" type="checkbox"/>	(h) We need it to comply with our legal obligations to provide or manage health or social care services
<input type="checkbox"/>	(i) We need it to comply with our legal obligations for public health
<input type="checkbox"/>	(j) We need it for archiving, research and statistics where this is in the public
<input type="checkbox"/>	Other
<input type="checkbox"/>	Not applicable

**13. What is the legal basis for sharing or using health and care data under the common law duty of confidentiality?**

<input checked="" type="checkbox"/>	<a href="#">Implied consent</a> [for individual care or local clinical or care audits]
-------------------------------------	--

## 14. How will the Parties ensure that information is safe and secure?

### Practice Responsibilities

The **practice** has robust local policies and procedures in place to ensure that patient information is handled **safely and securely**. These policies align with the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018**, and **NHS Digital standards**, ensuring full compliance with national guidelines.

#### Access Control & Auditing

- The **practice** has full control over **auditing user access**, including tracking logins by time and date.
- If a **generic PCIT user account** is identified, the practice can forward this information to PCIT to determine the individual responsible.
- **RBAC codes assigned to PCIT for operational needs include:**
  - o B1700
  - o B0994
- Comprehensive **audit logs** track all EHR activities to ensure full transparency.

#### Security & Compliance

- The **practice** ensures that access credentials are managed at the **organizational level**, allowing central control rather than individual-based restrictions.
- **No patient data is transferred** outside of the practice or to external systems—all information remains securely within the native **EHR environment**.

## PCIT Responsibilities

**Primary Care IT (PCIT)** provides technical support and security measures to assist practices in maintaining a secure environment.

### Access & Security Management

- PCIT follows **strict access control policies**, ensuring that access to practice systems is restricted to **authorized personnel only**.
- **PCIT does not hold or store patient data**—all information remains securely within the practice's native EHR environment.
- **Password changes** and access modifications are logged in **PCIT's internal management system**, recording both the action and the responsible individual.
- An **audit trail is maintained** to track all practice support requests, including access to practice login credentials by PCIT staff.

### Compliance & Risk Management

- PCIT's security policies align with **UK GDPR, the Data Protection Act 2018, and NHS Digital standards** to ensure compliance.
- PCIT is **ISO 27001 compliant**, demonstrating adherence to internationally recognized information security standards.
- Regular **audits and risk assessments** are conducted to identify and mitigate potential security vulnerabilities.

### Data Protection Measures

- PCIT implements **data encryption, access controls, and regular staff training** to safeguard sensitive information.
- Patient data is **only accessed when necessary to assist practices with issue resolution**.
- **PCIT does not transfer, store, or process patient data externally**—all actions are conducted within the practice's secure systems.

#### 15. For this Agreement, how long are the Parties planning to use the data for?

PCIT only uses the data for the duration of the specific support session or ticket raised by the GP practice. Data access is strictly limited to resolving the issue at hand, with no retention or prolonged use beyond the resolution of the support request.

#### 16. For this Agreement, how long do the Parties intend to keep the data?

PCIT does not retain any data. All data is accessed temporarily during the support session and is not stored or retained after the issue has been resolved.

**17. What will happen to the data at the end of this Agreement?**

Security measure	Details (leave blank if not applicable)
<input checked="" type="checkbox"/> The Controller(s) will manage as it is held by them	<p>The data is accessed temporarily and remains under the control of the GP practice system.</p> <p>At the end of the contract PCIT access to the clinical system will be removed by the Practice.</p>

**18. How will the Parties comply with the following data subject rights (where they apply)?**

Individual right	How the Parties will comply (or state <i>not applicable</i> if the right does not apply)
<p><b>The right to be informed</b> The right to be informed about the collection and use of personal data.</p>	<p>We have assessed how we should inform individuals about the use of data for PCIT supporting practices during this contract. We consider the communications methods below meet this obligation because these are reasonable and proportionate to the frequency and nature of the sharing</p> <p><input checked="" type="checkbox"/> Privacy notice(s) for all relevant organisations link provided on practice website</p> <p><input type="checkbox"/> Information leaflets</p> <p><input type="checkbox"/> Posters</p> <p><input type="checkbox"/> Letters</p> <p><input type="checkbox"/> Emails</p> <p><input type="checkbox"/> Texts</p>

	<input type="checkbox"/> Social media campaign <input checked="" type="checkbox"/> DPIA published (best practice rather than requirement) <input type="checkbox"/> Other <input type="checkbox"/> Not applicable
<b>The right of access</b> The right to access details of data use and receive a copy of their personal information - this is commonly referred to as a subject access request.	This is as per usual practice policies
<b>The right to rectification</b> The right to have inaccurate personal data rectified or completed if it is incomplete.	This is as per usual practice policies
<b>The right to erasure</b> The right to have personal data erased, if applicable	This is as per usual practice policies
<b>The right to restrict processing</b> The right to limit how their data is used, if applicable.	This is as per usual practice policies
<b>The right to data portability</b> The right to obtain and re-use their personal data, if applicable.	This is as per usual practice policies
<b>The right to object</b> The right to object to the use and sharing of personal data, if applicable.	This is as per usual practice policies

**19. Will the national data opt-out need to be applied? Which organisation is responsible for managing this process?**

<input type="checkbox"/>	Yes
<input checked="" type="checkbox"/>	No. The national data opt-out does not need to be applied  NDO will not apply to practice activity.  PCIT are not using the data, they are providing templates and infrastructure support for practice use and PCIT's use of data is strictly limited to direct care purposes and does not involve research or planning activities.

--

**20. List the organisation(s) that will decide why and how the data is being used and shared (Controllers).**

This will be the GP Practice (DUNCHURCH SURGERY).

**21. List the organisation(s) that are being instructed to use or share the data (Processors).**

Primary Care IT Ltd

**22. List any organisations that have been subcontracted by your Processor to handle data (Sub-Processors).**

N/A PCIT does not use Sub-Processors

**23. How will the Parties ensure data accuracy and that updates to the data are communicated where necessary?**

Practice staff are the only parties updating patient records and will follow all local and NHS guidelines.

By nature of the data being used for the purpose that it is being used for the PCIT team will only be accessing information in relation to where there are concerns about data accuracy in the first place. This will be done following contact by the practice with the PCIT support desk when a screen sharing session will be required for PCIT to investigation with the practice.

**24. Describe how data breaches will be managed.**

The Practice will follow its usual process for data breaches in line with NHS England requirements.

Where a data breach involves Primary Care IT, the practice will notify Primary Care IT as soon as it becomes aware of the breach. Primary Care IT will engage actively with the practice to investigate and report back to the practice. Primary Care IT should be notified via their support desk in the usual way.

**25. Set out any terms agreed by the Parties regarding liability.**

The practice has its own insurance.



The liabilities are covered in the contract with PCIT.

**26. If applicable, provide details of any agreed variation of terms from Part 2 of this agreement.**

N/A

**27. Set out the mechanism for issuing a variation to this agreement.**

This will be as agreed between the Parties.

**28. Detail any processing that has not been captured above.**

N/A

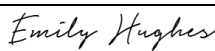
**29. Set out the review period for this agreement.**

The practice will review this in line with their current policies.


PCIT will advise if there are any changes identified which would impact on this agreement.

**30. Signatories**

**Authorised signatory on behalf of the Controller**

Name	Role	Organisation	Signature	Date
Emily Hughes	Practice Manager	DUNCHURCH SURGERY		26 Feb 202

**Authorised signatory on behalf of the Processor**

Name	Role	Organisation	Signature	Date
Dustyn Saint	Founder/CEO	Primary Care IT		26 Feb 2025

Part 1 Annex 1 – List of Controllers and Processors and their  
named points of contact

Name	Role	Organisation	Contact
Emily Hughes	Controller	DUNCHURCH SURGERY	emily.hughes@nhs.net
Brandon Crisp	Processor	Primary Care IT	brandon@primarycareit.co.uk

## Part 2

### 1. BACKGROUND AND SCOPE

- 1.1. This Part 2 of this Agreement sets out the general terms and conditions relating to inter-Party Data Processing Activities which the Parties agree to meet.
- 1.2. Part 1 of the Agreement sets out the specific details of what each Party has agreed to in respect of any intended inter-Party Processing of Personal Data.
- 1.3. The Parties agree that no Party will access or otherwise Process Personal Data that solely relates to any other Party's individual Processing purpose, which is outside of the scope of the Processing set out in Part 1 of the Agreement.
- 1.4. To the extent that any other agreement between the Parties in relation to these Data Processing activities contains any provisions which govern the Processing of Personal Data by the Parties, the Parties agree and acknowledge that the provisions of this Agreement shall prevail in the event of any conflict or inconsistency.
- 1.5. Data Protection Legislation requires that "[w]here two or more controllers jointly determine the purposes and the means of Processing they shall be joint controllers." It also requires that Joint Controllers determine their respective responsibilities for compliance "...in a transparent manner...by means of an arrangement between them..." This Agreement meets the requirement of having an arrangement. All Parties shall meet the additional transparency requirements under clause 13.

**IT IS AGREED** as follows:

### 2. DEFINITIONS AND INTERPRETATION

- 2.1. The following definitions shall apply in this Agreement:

**Commencement Date** means between any two Parties or more the date from which the last of those Parties have signed this Agreement in respect of any Data Processing Activities (or such other date as those Parties may agree);

**Controller** means a 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;

**Data Guidance** means any applicable guidance, guidelines, direction or determination, framework, code of practice, standard or requirement regarding information governance, confidentiality, privacy or compliance with the Data Protection Legislation (whether specifically mentioned in this Agreement or not) to the extent published and publicly available or their existence or contents have been notified to the Parties by NHS England and/or any relevant Regulatory, Advisory or Supervisory Body. This includes but is not limited to guidance issued by the National Data Guardian for Health and Care, the Department of Health and Social Care, NHS England, the Health Research Authority, Public Health England (now the UK Health Security Agency) and the Information Commissioner;

**Data Loss Event** means any event that results, or may result, in unauthorised Processing of Personal Data held by the Parties under this Agreement or the loss of Personal Data that the Parties have responsibility for under this Agreement including without limitation actual or potential loss, destruction, corruption or inaccessibility of Personal Data, including any Personal Data Breach;

**Data Processing Activities** means the data Processing activities described in Part 1 of this Agreement;

**Data Protection Impact Assessment (DPIA)** means an assessment by the Controller(s) of the impact of the envisaged Processing on the protection of Personal Data;

**Data Protection Legislation** means UK Data Protection legislation currently comprising (i) the DPA 2018 (ii) the UK GDPR, the Law Enforcement Directive and any applicable national Laws implementing them as amended from time to time (iii) all applicable Law concerning privacy, confidentiality or the Processing of personal data including but not limited to the Human Rights Act 1998, the Common Law Duty of Confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations 2003;

**Data Protection Officer (DPO)** shall be the individual designated as such by Controllers and Processors where required by the Data Protection Legislation;

**Data Subject** means an identified or identifiable natural person whose Personal Data is being Processed;

**DPA 2018** means the Data Protection Act 2018;

**EU** means the European Union;

**Information Commissioner** means the Information Commissioner's Office ([ICO](#)) which is the independent authority established to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals and any other relevant data protection or supervisory authority recognised pursuant to the Data Protection Legislation;

**International Data Transfer Agreement (IDTA)** means the documents approved for the restricted transfer of Personal Data to countries not covered by UK adequacy regulations. The documents can be found on the [Information Commissioner's website](#);

**Joint Controller** means where two or more Controllers jointly determine the purposes and means of Processing;

**Law** means any law or subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, by-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgement of a relevant court of law, or directives or requirements with which the Parties are bound to comply;

**LED** means the Law Enforcement Directive (Directive (EU) 2016/680);

**Party or Parties** shall mean any and all signatories to this agreement, including Controllers and Processors and signatories acting as Sub-Processors;

**Personal Data** means any information relating to an identified or identifiable natural person. 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;

**Personal Data Breach** shall take the meaning given in the Data Protection Legislation, and shall also include events that would have been regarded as Personal Data Breach but which relate to information about deceased individuals where a duty of confidentiality is still owed;

**Processor** means a natural or legal person, public authority, agency or other body which Processes personal data on behalf of a Controller or (where a Party to this Agreement this shall include Processors acting as Sub-Processors, provided that the relevant Processing is described Part 1 of this Agreement). A Controller may instruct a Processor who is not a Party to this Agreement, provided such contractual provisions as are required by the Data Protection Legislation are in place with such a Processor;

**Processing** and cognate terms mean 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;

**Protective Measures** means appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data; ensuring confidentiality, integrity, availability and resilience of systems and services; ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident; and regularly assessing and evaluating the effectiveness of such measures;

**Regulatory or Supervisory Body** means any statutory or other body having authority to issue guidance, standards or recommendations with which the Parties and/or their staff must comply or have regard to, including:

- (i) The Care Quality Commission (CQC);
- (ii) NHS England;
- (iii) the Department of Health and Social Care;
- (iv) the National Institute for Health and Care Excellence;
- (v) Healthwatch England and Local Healthwatch;
- (vi) UK Health Security Agency;
- (vi) The General Medical Council
- (vii) The General Dental Council
- (viii) The Nursing and Midwifery Council
- (ix) the General Pharmaceutical Council;
- (x) the Healthcare Safety Investigation Branch; or
- (xi) the Information Commissioner.

**Respective Responsibilities** means for each Controller who is a Joint Controller the responsibilities which must, in a transparent manner, be determined for compliance with the Data Protection Legislation

**Responsible Controller** means (i) in the event of a Personal Data Breach by a Processor, the Controller who instructed that Processor (ii) in the event of a Personal Data Breach by a Controller, that Controller (iii) where Joint Controllers have designated one party as the Responsible Controller in relation to the relevant Personal Data Breach under the Agreement, that designated Controller, (iv) where there is no agreement then each of the Joint Controllers shall be a Responsible Controller;

**Staff** means any and all persons employed or engaged from time to time in the provision of the Data Processing Activities whether employees, workers, consultants or agents of any Party or any subcontractor or agent of any Party;

**Subject Rights Request** means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation including to access their Personal Data (including a “subject access request”);

**Sub-Processor** means any organisation appointed by a Processor to Process Personal Data on behalf of a Processor;

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

**Working Day** means a day other than a Saturday, Sunday, or public or bank holiday in England.

- 2.2. The following rules of interpretation shall apply to this Agreement:
- reference to any legislative provision shall be deemed to include any statutory instrument, by-law, regulation, rule, subordinate or delegated legislation or order and any rules and regulations which are made under it, and any subsequent re- enactment, amendment or replacement of the same;
  - 2.2.1. words in the singular shall include the plural and in the plural shall include the singular; and
  - 2.2.2. references to clauses and Annexes are to clauses and Annexes to this Agreement.

### 3. DURATION AND CONSIDERATION

- 3.1. This Agreement shall commence on the Commencement Date and shall continue until termination or expiry for whatever reason.
- 3.2. This Agreement is entered into in consideration of the mutual trust, convenience and benefit of all the Parties and in consideration of the benefits to the health and care system.

### 4. GENERAL OBLIGATIONS

- 4.1. A Controller remains legally responsible for the Personal Data where it is being Processed by a Processor and therefore the Controller must take steps to ensure the information assets remain protected and that the liabilities and risk are appropriately managed, Personal Data is Processed lawfully, and the Agreement is legally enforceable.

- 4.2. A Processor is nevertheless also legally responsible for the Personal Data to the extent required under Data Protection Legislation and in any relevant Personal Data Processing contract.
- 4.3. Each Party shall ensure that it has in place Protective Measures in relation to the Personal Data Processed under this Agreement, which are appropriate to protect against a Data Loss Event having taken account of the:
  - 4.3.1. nature of the Personal Data to be protected;
  - 4.3.2. harm that might result from a Data Loss Event;
  - 4.3.3. state of technological development; and
  - 4.3.4. cost of implementing any measures;

Processors who are Party to this Agreement are subject to additional requirements under clause 6.7.2. Where a Controller instructs a Processor who will Process Personal Data in relation to this Agreement and such Processor is not a Party to this Agreement, the instructing Controller shall ensure that contractual provisions complying with the Data Protection Legislation are in place with such Processor.

- 4.4. Each Party shall ensure that its staff involved in the Processing of Data under this Agreement have undergone adequate training in the use, care, protection and handling of Personal Data that enables them and the Processor to comply with their responsibilities under the Data Protection Legislation and this Agreement. Processors are subject to additional requirements under clause 6.7.3.
- 4.5. All Parties shall in good faith cooperate fully during any handover arising from the cessation of any part of the Data Processing Activities. Processors are subject to additional requirements under clause 6.7.7.
- 4.6. All Parties shall be under a duty to notify any potentially impacted Parties where they become aware of or reasonably suspect a Data Loss Event; or become aware of or reasonably suspect that it has in any way caused, or might reasonably be considered to be likely to cause, a breach of Data Protection Legislation by another Party. Processors are subject to additional requirements under clause 6.8.

## **5. CONTROLLER OBLIGATIONS**

- 5.1. Each Controller shall at all times ensure Personal Data is Processed fairly, lawfully and transparently in accordance with Data Protection Legislation.
- 5.2. Each Controller warrants that any instructions it issues to a Processor in respect of the Personal Data are lawful.



## **6. ADDITIONAL ALL PARTY AND PROCESSOR SPECIFIC OBLIGATIONS**

- 6.1. The following obligations within this clause 6 shall apply where at least one Processor has been identified in Part 1 of this Agreement. Where the Processor is not a Party to this Agreement, the Controllers who instruct them must ensure that any contracts with such Processors provide equivalent protection to the clauses set out in clause 6 of this Agreement. Where indicated, the obligations shall apply to any Party to this Agreement not just Processors.
- 6.2. The Parties acknowledge that for the purposes of the Data Protection Legislation in relation to the Data Processing Activities, the Controller(s) and the Processor(s) are as set out in Part 1 of this Agreement. A Processor must Process the Processor Data only to the extent necessary to perform the Data Processing Activities and only in accordance with the written instructions set out in Part 1 of this Agreement.
- 6.3. A Processor must use the Personal Data shared solely for the purposes as instructed and shall not Process the Personal Data for any other purposes.
- 6.4. Each Party agrees to treat the data (including Personal Data) received by them under the terms of this Agreement as confidential and shall safeguard it accordingly.
- 6.5. All Parties must provide all reasonable assistance to one another and in particular to any Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing under this Agreement. Such assistance may include:
  - 6.5.1.a systematic description of the envisaged Processing operations and the purpose of the Processing;
  - 6.5.2.an assessment of the necessity and proportionality of the Processing operations in relation to the Data Processing Activities;
  - 6.5.3.an assessment of the risks to the rights and freedoms of Data Subjects; and
  - 6.5.4.the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
- 6.6. Any Party requested, but in particular any Processor who is a Party to this Agreement, shall provide all reasonable assistance to a Controller if the outcome of the Data Protection Impact Assessment leads the Controller to consult the Information Commissioner concerning any proposed arrangements.

6.7. A Processor must (and must be required in any contractual documentation where such Processor is not a Party to this Agreement), in relation to any Personal Data Processed in connection with its obligations under this Agreement:

6.7.1. Process that Personal Data only in accordance with the documented instructions of a Controller, unless the Processor is required to do otherwise by Law. If it is so required, the Processor must promptly notify the Controller before Processing the Personal Data unless such notification is prohibited by Law;

6.7.2. ensure that it has in place Protective Measures, which have been reviewed and approved by the Controller as appropriate to protect against a Data Loss Event having taken account of the:

6.7.2.1. nature of the Personal Data to be protected;

6.7.2.2. harm that might result from a Data Loss Event;

6.7.2.3. state of technological development; and

6.7.2.4. cost of implementing any measures;

6.7.3. ensure:

6.7.3.1. when delivering the Data Processing Activities, the Processor Staff only Process Personal Data in accordance with this Agreement;

6.7.3.2. it takes all reasonable steps to ensure the reliability and integrity of any Processor Staff who have access to the Personal Data and ensure that they:

6.7.3.2.1. are aware of and comply with the Processor's duties under this clause;

6.7.3.2.2. are subject to appropriate confidentiality undertakings with the Processor and any Sub-Processor that are in writing and are legally enforceable;

6.7.3.2.3. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and

6.7.3.2.4. have undergone adequate training in the use, care, protection and handling of Personal Data that enables them and the Processor to comply with their responsibilities under

the Data Protection Legislation and this Agreement. The Processor shall provide the Controller with evidence of completion and maintenance of that training within three Working Days of request by the Controller.

- 6.7.4. at the written direction of the Controller, delete or return Personal Data (and any copies of it) to that Controller on termination of the Data Processing Activities and certify to the Controller that it has done so within five Working Days of any such instructions being issued, unless the Processor is required by Law to retain the Personal Data;
  - 6.7.5. if the Processor is required by any Law or Regulatory or Supervisory Body to retain any Processor Data that it would otherwise be required to destroy under this clause 6, notify the Controller in writing of that retention giving details of the Processor Data that it must retain and the reasons for its retention;
  - 6.7.6. notify the Controller immediately if it considers that carrying out any of the Controller's instructions would infringe Data Protection Legislation. This obligation extends to breaches concerning the systems on which the data shared under this Agreement are held, even if the data shared under this Agreement is not directly affected;
  - 6.7.7. cooperate fully with the Controller during any handover arising from the cessation of any part of the Data Processing Activities, and if the Controller directs the Processor to migrate Processor Data to the Controller or to another nominated organisation, provide all reasonable assistance with ensuring safe migration including ensuring the integrity of Personal Data and the nomination of a named point of contact for the Controller (as set out in Annex 1 of Part 1 of this Agreement).
- 6.8. Subject to clause 6.10, a Processor must notify the relevant Controller immediately if it:
- 6.8.1. receives a Subject Rights Request (or purported Subject Rights Request);
  - 6.8.2. receives a request to rectify, block or erase any Personal Data;
  - 6.8.3. receives any other request, complaint or communication relating to obligations under Data Protection Legislation owed by the Processor or Controller;
  - 6.8.4. receives any communication from the Information Commissioner or any other Regulatory or Supervisory Body (including any communication concerned with the systems on which Personal Data is Processed under this Agreement);

- 6.8.5. receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law;
  - 6.8.6. becomes aware of or reasonably suspects a Data Loss Event; or
  - 6.8.7. becomes aware of or reasonably suspects that it has in any way caused the Controller to breach Data Protection Legislation.
- 6.9. The notification under clause 6.8 shall be given by emailing any relevant request and any subsequent communications to the Controller's Data Protection Officer immediately, and in no longer than one Working Day of receipt by the Processor.
- 6.10. A Processor shall not respond substantively to the communications listed at clause 6.8 save that it may respond to a Regulatory or Supervisory Body following prior consultation with the Controller.
- 6.11. A Processor's obligation to notify under clause 6.8 includes the provision of further information to the Controller in phases, as details become available.
- 6.12. A Processor must provide their instructing Controller with all reasonable assistance in relation to either Party's obligations under the Data Protection Legislation and any complaint, communication or request made under clause 6.8 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:
- 6.12.1. the Controller with full details and copies of the complaint, communication or request;
  - 6.12.2. the Controller with any Personal Data it holds in relation to a Data Subject;
  - 6.12.3. such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Subject Rights Request within the relevant timescales set out in the Data Protection Legislation;
  - 6.12.4. such assistance as is reasonably requested by the Controller to enable the Controller to comply with other rights granted to individuals by the Data Protection Legislation including the right of rectification, the right to erasure, the right to object to Processing, the right to restrict Processing, the right to data portability and the right not to be subject to an automated individual decision (including profiling);
  - 6.12.5. assistance as requested by the Controller following any Personal Data Loss Event;

- 6.12.6. assistance as requested by the Controller in relation to informing a Data Subject about any Data Loss Event, including communication with the Data Subject;
  - 6.12.7. assistance as requested by the Controller with respect to any request from the Information Commissioner, or any consultation by the Controller with the Information Commissioner.
  - 6.12.8. A Processor shall designate a Data Protection Officer if required by the Data Protection Legislation, and shall communicate to the Controller the name and contact details of any Data Protection Officer.
- 6.13. A Processor must allow for reasonable audits of its delivery of the Data Processing Activities by the Controller or the Controller's designated auditor at no additional cost to the Controller.
- 6.14. For the avoidance of doubt:
- 6.14.1. a Processor must not novate this Agreement nor assign, delegate, subcontract, transfer, charge or otherwise dispose of all or any of its rights or obligations or duties under this Agreement without the prior written approval of the instructing Controller. The approval of any sub-processing or subcontracting arrangement may include approval of the terms of the proposed subcontract;
  - 6.14.2. subcontracting any part of this Agreement will not relieve a Processor of any of its obligations or duties under this Agreement. A Processor will be responsible for the performance of and will be liable to the Controller for the acts and/or omissions of all Sub-Processors as though they were their own;
  - 6.14.3. any positive obligation or duty on the part of the Processor under this Agreement includes an obligation or duty to ensure that all subcontractors and Sub-Processors comply with that positive obligation or duty. Any negative duty or obligation on the part of the Processor under this Agreement includes an obligation or duty to ensure that all subcontractors and Sub-Processors comply with that negative obligation or duty.
- 6.15. Without prejudice to clause 6.16, before allowing any Sub-Processor to Process any Personal Data related to this Agreement, a Processor must:
- 6.15.1. notify the relevant Controller in writing of the intended Sub-Processor and Processing;
  - 6.15.2. obtain the written consent of the relevant Controller;
  - 6.15.3. carry out appropriate due diligence of the Sub-Processor and ensure this is documented;

- 6.15.4. enter into a binding written agreement with the Sub-Processor which includes equivalent terms to those set out in this Agreement; and
    - 6.15.5. provide the relevant Controller with such information regarding the Sub-Processor as the Controller may reasonably require.
  - 6.16. The Parties agree to take account of any guidance issued by the Information Commissioner. A Controller may (or where there is more than one Controller they may by agreement) on not less than 30 Working Days' notice to the Processor amend this Agreement to ensure that it complies with any guidance issued by the Information Commissioner.
  - 6.17. A Controller may (or where there is more than one Controller they may by agreement), at any time on not less than 30 Working Days' notice, revise this Agreement by adding to it any applicable Controller to Processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).
  - 6.18. A Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Agreement, the Data Protection Legislation and Data Guidance. A Processor must create and maintain a record of all categories of data Processing activities carried out under this Agreement, which must be made available to the instructing Controller within two Working Days of a written request, containing:
    - 6.18.1. the categories of Processing carried out under this Agreement;
    - 6.18.2. details of categories of Data Subjects;
    - 6.18.3. where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, where relevant, the documentation of suitable safeguards;
    - 6.18.4. a general description of the Protective Measures taken to ensure the security and integrity of the Personal Data Processed under this Agreement; and
    - 6.18.5. a log recording the Processing of Personal Data in connection with this Agreement comprising, as a minimum, details of the Personal Data concerned, how the Personal Data was Processed, where the Personal Data was Processed and the identity of any individual carrying out the Processing.
  - 6.19. A Processor warrants and undertakes that it will deliver the Data Processing Activities in accordance with the Data Protection Legislation and this Agreement and in particular that it has in place Protective Measures that are sufficient to ensure that the delivery of the Data Processing Activities complies

with the Data Protection Legislation and ensures that the rights of Data Subjects are protected.

- 6.20. A Processor must assist the Controller in ensuring compliance with the obligations set out at Article 32 to 36 of the UK GDPR and equivalent provisions implemented into Law, taking into account the nature of Processing and the information available to the Processor.
- 6.21. A Processor must assist the Controller in ensuring compliance with the obligations set out in Articles 32 to 36 of the UK GDPR (security of Processing, obligations with regards to Personal Data Breaches and conducting Data Protection Impact Assessments) and equivalent provisions implemented into Law, taking into account the nature of Processing and the information available to the Processor.
- 6.22. A Processor must take prompt and proper remedial action regarding any Data Loss Event.
- 6.23. A Processor must assist the Controller by taking appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controllers' obligation to respond to requests for exercising rights granted to individuals by Data Protection Legislation.
- 6.24. A Processor must promptly (and in any event within a maximum of four (4) Working Days) comply with any request of the Controller or the Information Commissioner to provide a copy of any or all Personal Data which is under the Processor's custody or control, in the format and on a media reasonably specified by the Controller or the Information Commissioner.
- 6.25. A Processor must not transfer Personal Data outside the UK except to countries covered by adequacy regulations, unless the prior written consent of their instructing Controller has been obtained and the following conditions are fulfilled:
  - 6.25.1. appropriate safeguards in relation to the transfer are in place as determined by the instructing Controller;
  - 6.25.2. the Data Subject has enforceable rights and effective legal remedies;
  - 6.25.3. the Party transferring the data complies with its obligations under Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the relevant Controller in meeting its obligations); and
  - 6.25.4. the Processor, where one has been appointed, complies with any reasonable instructions notified to it in advance by the relevant Controller with respect to the Processing of the Personal Data.

## 7. PERSONAL DATA BREACHES

- 7.1. A Responsible Controller will notify the other Controllers who are Parties to this Agreement of a Data Breach if, acting reasonably, they consider that the interests of those Controllers may be affected by any Personal Data Breach for which it is the Responsible Controller. In the case of Joint Controllers, each of the Joint Controllers shall notify the other Joint Controllers of any Personal Data Breach of which it becomes aware.
- 7.2. A Responsible Controller will determine whether to notify Personal Data Breaches to the Information Commissioner.
- 7.3. A Responsible Controller will determine whether and how to notify Personal Data Breaches to the Data Subjects.
- 7.4. The Responsible Controller will monitor Personal Data Breach responses to ensure compliance with statutory timescale and any other requirements arising by Law or under this Agreement.

## 8. DATA SECURITY ARRANGEMENTS

- 8.1. All Parties shall:
  - 8.1.1. have in place appropriate technical and organisational security measures designed to protect Personal Data against accidental events or unlawful or malicious actions that compromise the availability, integrity and confidentiality of the Personal Data, and ensure that such measures are appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Personal Data and have regard to the nature of the Personal Data which is to be protected;
  - 8.1.2. ensure that all Personal Data Processed by any Party and its staff are subject to the technical and organisational security measures the Party implements and maintains, pursuant to clause 8.1.1 above;
  - 8.1.3. have procedures in place to monitor access to the Personal Data and to identify unauthorised and unlawful access and use of Personal Data;
  - 8.1.4. where health and care data is accessed by a Party, that Party must complete and publish an annual information governance assessment in accordance with, and comply with the mandatory requirements of, the NHS Data Security and Protection Toolkit, as applicable to the Data Processing Activities and the Party's organisation type. Where health and care data is not accessed, any Party accessing other Personal Data must maintain annual governance assessments to any agreed equivalent standard; and



8.2. A Processor shall:

- 8.2.1. immediately report any untoward incidents, near misses or activities that suggest non-compliance with this Agreement to the Controller and cooperate with the Controller to carry out a risk assessment, root cause analysis and identify any corrective action required. A Processor will cooperate with the Controller in implementing any required corrective action agreed between the Parties. (N.B. It is the Controller's responsibility to ensure that any incidents are reported in accordance with the Department of Health and Social Care policy and procedures and for informing the relevant Data Subjects as appropriate.)

## 9. LIABILITY

- 9.1. The Parties shall not do or omit to do anything that will put any other Party in breach of the Data Protection Legislation or the Data Guidance.
- 9.2. The rights and remedies provided under Part 1 of this Agreement are in addition to, and not exclusive of, any rights or remedies provided by Law or in equity.
- 9.3. A waiver of any right or remedy under Part 1 of this Agreement or by Law or in equity is only effective if given in writing and signed on behalf of the Party giving it and any such waiver so given shall not be deemed a waiver of any similar or subsequent breach or default.
- 9.4. A failure or delay by a Party in exercising any right or remedy provided under Part 1 of this Agreement or by Law or in equity shall not constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict any further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy provided under this Agreement or by Law or in equity shall prevent or restrict the further exercise of that or any other right or remedy.

## 10. VARIATION OF AGREEMENT

- 10.1. Any proposed changes to this Agreement, including the addition or removal of parties, the purposes of the information sharing, the nature or type of information shared or manner in which the information is to be Processed must be notified promptly to the Information Compliance/Governance leads so that the impact of the proposed changes can be assessed.
- 10.2. No variation of this Agreement shall be effective unless it is in writing and signed by all Parties to this Agreement.

## **11. FREEDOM OF INFORMATION AND ENVIRONMENTAL INFORMATION REGULATIONS**

- 11.1. Where a Controller is a public authority, the Parties acknowledge that such a Controller is subject to the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR).
- 11.2. A Controller as set out in clause 11.1 will be statutorily required, subject to any applicable exemptions, to disclose information about the Data Processing Activities provided under this Agreement or the Agreement itself in response to a specific request under FOIA or EIR. In which case:
- 11.2.1. A Processor shall provide its instructing Controller with all reasonable assistance and co-operation to enable the Controller to comply with its obligations under FOIA or EIR; and
- 11.2.2. A Controller as set out in clause 11.1 Controller shall consult any Party it reasonably considers relevant or who may have a legitimate interest in respect of any commercial, confidential or other issues in relation to the Agreement relevant to the issue of whether the information is exempt from disclosure or not; however the final decision about disclosure of information or application of exemptions shall rest solely with the Controller which has received the request.

## **12. GENERAL**

- 12.1. A Processor, where appointed, shall not assign, transfer, mortgage, charge, subcontract, declare a trust over or deal in any other manner with any or all of its rights and obligations under this Agreement without the prior written consent of their instructing Controller.
- 12.2. This Agreement may be executed in any number of counterparts, each of which when executed and delivered shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement.
- 12.3. It is an offence under the Data Protection Legislation for any Party to knowingly or recklessly re-identify any data that is de-identified without the consent of the Controller that has provided the information.

## **13. TRANSPARENCY**

- 13.1. All Parties agree that the Controllers shall:
- 13.1.1. ensure publication of a summary of the Data Processing Activities, provided in a concise, transparent, intelligible and easily accessible form;

13.1.2. ensure Data Subjects are appropriately instructed on how they can exercise their rights under Data Protection Legislation, including where they must contact another Party; and

13.1.3. to reference other Parties' transparency materials published under 13.1.1.

## **14. DISPUTE RESOLUTION**

14.1. Parties shall aim to resolve all disputes, differences and questions by means of cooperation and consultation.

14.2. If any dispute arises, the Parties in dispute must first attempt to settle it with a written offer of negotiation by any of the Parties to the other Parties. During the following 15 Business Days Period each of the Parties in dispute must negotiate and be represented:

14.2.1. for the first 10 Business Days, by a senior person who where practicable has not had any direct day-to-day involvement in the matter and has authority to settle the Dispute; and

14.2.2. for the last 5 Business Days, by their chief executive, director, or equivalent senior individual who has authority to settle the dispute.

14.3. Where practicable, no Party in dispute should be represented by the same individual for the different stages described in 14.2.1 and 14.2.2 above.

14.4. If the Parties in dispute are unable to settle the Dispute by negotiation, they must, within 5 Business Days after the end of the Negotiation Period, submit the Dispute to mediation by the Centre for Effective Dispute Resolution (CEDR) or other independent body or organisation agreed between the Parties which will follow the mediation Process of CEDR or other independent body or organisation as agreed.

14.5. This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the Law of England.

14.6. Each Party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Agreement or its subject matter or formation (including non-contractual disputes or claims), provided that nothing in this clause shall prevent a Party from enforcing any judgement obtained in the court of England and Wales in any other court with jurisdiction over the other Party.

## **15. TERMINATION**

- 15.1. These arrangements may be terminated in respect of a Party by that Party giving reasonable notice to the other Parties. Termination by one Party shall not terminate the Agreement in respect of the other Parties.
- 15.2. The Parties may terminate this Agreement by mutual agreement.
- 15.3. Without affecting any other right or remedy available to it, a Controller may immediately terminate this Agreement by notice in writing to a Processor if the Processor commits a material breach of any provision of this Agreement, or the Processor repeatedly breaches any of the provisions of this Agreement.