**[V2 – 25/09/2019]**

# Joint Controller and Information Sharing Framework Agreement

**Between**

**Monitor (1)**

**And**

**The National Health Service Trust Development Authority (2)**

**And**

**The NHS Commissioning Board (3)**

# Table of Contents

This agreement (the Agreement) is made between:

MONITOR;

THE NATIONAL HEALTH SERVICE TRUST DEVELOPMENT AUTHORITY ("the TDA"),

Parties (1) and (2) together known as NHS IMPROVEMENT; and

THE NATIONAL HEALTH SERVICE COMMISSIONING BOARD ("NHS England"),

each of (1), (2) and (3) being a "Party" and together referred to as "the Parties".

## 1. Background

(A) Monitor and the TDA (a Special Health Authority) have come together under the operational name NHS Improvement, combining the functions and responsibilities of the two statutory bodies in a single integrated organisation. NHS Improvement is responsible, among other things, for the oversight of NHS trusts and NHS foundation trusts and the assessment of certain transactions into which such bodies may enter.

(B) NHS England is responsible, among other things, for the commissioning of NHS health services and the oversight of clinical commissioning groups.

(C) Monitor and the TDA already have in place arrangements to work collaboratively together under a single leadership and operating model as NHS Improvement, to ensure improvement in quality of care, patient safety and financial sustainability across the health service[1].

(D) The Parties have duties to cooperate with each other under section 290 of the Health and Social Care Act 2012 (the "2012 Act") and section 72 of the National Health Service Act 2006 ("the 2006 Act"), and each has its own powers, and is subject to duties, to work collaboratively.

(E) The Parties are entering into a Memorandum of Understanding on co-operation by which they agree to work collaboratively to deliver a new model of joint working.

(F) The Parties are to work collaboratively, share information and Process personal data jointly with one another pursuant to, in particular, their respective duties and powers under sections 62 and 290 of, and paragraph 15 of Schedule 8, to the 2012 Act and sections 2 and 72 of, and directions under, sections 7 and 8 of, the 2006 Act.

(G) Recognising that the pursuit of the Parties' shared objectives will entail cooperation between the Parties in the exercise of their functions, and that this will in turn require the Parties to put in place measures to ensure that, in relation to any personal data that is

---

1 See direction 2(1) of the NHS TDA Directions and Revocations and the Revocation of the Imperial College Healthcare National Health Service Trust Directions 2016

Processed in the cooperative exercise of their functions, good information governance is maintained and that the Parties comply with Data Protection Law, this Agreement and the Memorandum of Understanding on co-operation which set out arrangements for the Parties to collaborate in respect of information governance.

(H) Each of the Parties is and will remain a separate legal entity, each having been created by statute to perform the functions conferred on them. The Parties will, notwithstanding the cooperative exercise of their functions, be individually subject to the obligations placed on them by Data Protection Law and accountable for the activities that they undertake in relation to the Processing of personal data.

(I) The purpose of this Agreement is to set out the responsibilities of the Parties when they are acting as joint controllers or sharing personal data as individual controllers.

(J) The Agreement outlines the shared information governance arrangements that the Parties will establish and maintain, including the appointment of a single Data Protection Officer.

(K) The Parties agree to enter into this Agreement, and by observing its provisions the Parties will ensure that the requirements of the law and good information governance are followed in the pursuit of their cooperative exercise of their functions.

## 2. Commencement and Duration

This Agreement shall commence on the 12th March 2019 and shall continue until brought to an end in accordance with clause 20.1.

## 3. Definitions

The following terms:

- “Data”, “personal data” and “special category data”;
- “Controller”;
- “Processor”;
- “Data subject”;
- “DPIA”, data processing impact assessment,
- “Data Protection Officer/DPO”;
- “Personal data breach”; and
- “Processing” (in the context of activities carried out in relation to personal data)

have the meaning given to them in Data Protection Law.

"Data Protection Law" means the General Data Protection Regulation (Regulation (EU) 2016/679) and the Data Protection Act 2018, together with any subordinate legislation made under the Act.

## 4. Purpose of the Agreement

4.1 The purpose of this agreement is to set out the responsibilities of the Parties when they act either as individual Controllers which share personal data or as joint Controllers. Setting out these responsibilities and subsequently making specific arrangements that put them into effect will assist the Parties to:

(a) understand their respective responsibilities and the actions they need to take to comply with Data Protection Law; and

(b) achieve their respective duties to cooperate under section 290 of the 2012 Act and section 72 of the 2006 Act and help to deliver the seamless integration of the exercise of their respective functions.

4.2 The General Data Protection Regulation 2016 (GDPR) says 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 sets out how the Parties intend to meet this requirement.

4.3 The GDPR further requires that the arrangement *"…shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject."* Section 6 presents the essence of this Agreement. The Parties will include this statement in the privacy information that they provide to Data subjects.

## 5. Scope of the Agreement

5.1 The scope of the Agreement is the Processing of personal data that is necessary for the joint working purposes that the Parties are committing to and which will be included in the Memorandum of Understanding on co-operation.

5.2 The Parties may additionally enter into arrangements as to the cooperative use of information other than personal data or special category data outside the scope of this Agreement.

5.3 Any documentation entered into between the Parties concerning their cooperative use of personal data (i.e. standard operating procedures, information sharing agreements or

data processing agreements as applicable) may additionally make provision in respect of the cooperative use of information other than personal data or special category data.

5.4 The commitment to cooperation in information governance establishes the requirement for this Agreement, and the supporting activities that are addressed in this Agreement.

## 6. Roles of the Parties in relation to data subjects

6.1 The essence of this Agreement is to enable the Parties to work together seamlessly in establishing their joint enterprise, ensuring that activities that involve the Processing or personal data are transparent and that the Parties comply with their data protection obligations.

6.2 The Parties are cooperating to establish a joint enterprise. This mirrors the focus of the NHS Long Term Plan on how the Parties will deliver integrated care to patients at the local level, how they set the whole of the NHS up to do that and how it will benefit patients and communities. Drawing together the Parties' people and capabilities, resources, activities and leadership means they can have more impact on patient care.

6.3 To make this work the Parties will need to perform some functions of individual organisations together, achieving seamless integration of their working practices. When the Parties use personal data for their joint purposes they will comply with Data Protection Law, sometimes as joint Controllers of that data.

6.4 This Agreement provides a framework for how the Parties will work together to ensure that they comply with Data Protection Law.

6.5 The Parties' data protection commitments as joint Controllers are set out below:

- the Parties will make sure that they are transparent about their joint purposes for Processing personal data, and explain how data is used for these purposes;
- the Parties will make sure that anyone who wants to have access to their personal data, or to exercise other legal rights, has an easily accessible point of contact to make their request;
- the Parties will make sure that when they introduce new joint working practices, the privacy of the people whose information are held by the Parties will continue to be protected as necessary;
- the Parties will only introduce new joint working practices after they have conducted an assessment of how they will comply with data protection legislation and this has been approved following a jointly agreed approval process; and
- the Parties will make sure that their data protection policies properly govern the activities of the joint enterprise, and that staff have a confident understanding of their responsibilities.

## 7. The Parties as sole Controllers and joint Controllers

7.1 This clause describes the circumstances in which the Parties may Process personal data as joint or sole Controllers for the purposes that they are committing to as part of Joint Working.

7.2 The GDPR defines a Controller as

> *"…the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data…"*

7.3 The Parties are statutory bodies and public authorities under Data Protection Law. As such they are subject to administrative (public) law and may only act within their statutory powers. The exercise of the Parties' individual functions cannot be shared or delegated unless specifically allowed for by legislation. So, when establishing collaborative activities in relation to those functions, the Parties individually must determine whether they have the power to perform the proposed activity and the lawful basis for any data sharing and Processing. Where the Parties work together in the exercise of their statutory functions, and in doing so jointly determine the purposes and means of Processing any personal data, they will be acting as joint Controllers.

7.4 The Parties also undertake a wide range of incidental or ancillary activities in order to operate effectively and support the discharge of their respective statutory functions. Activities relating to workforce management are an example. Where the Parties Process personal data for the joint exercise of such functions, and in doing so jointly determine the purposes and means of Processing any personal data, they will be acting as joint Controllers.

7.5 Where one Party Processes personal data in the exercise of its own functions only, it alone is responsible for determining the purpose and means of Processing and consequently it is the sole Controller. In this case, an employee of another of the Parties who assists with the Processing under the guidance, direction or supervision of the sole Controller is acting as an agent of the Party which has the function, and which is the Controller. This situation may arise, for example, in a reciprocal arrangement where the Parties have equivalent but separate functions, delivered by a jointly managed department. An example of this is the Processing of Data subjects' rights requests by the Corporate Information Governance team which is staffed by employees of all of the Parties working under the management of the Data Protection Officer, who is jointly employed by the Parties.

7.6 Any Party which Processes Personal Data for its own purposes may share that Personal Data with any of the other Parties, provided such sharing is lawful, on the grounds that it would assist the receiving Party to have access to that Personal Data for the purposes of

carrying out its own work. In this scenario, information is shared between separate and sole Controllers for their own individual purposes.

7.7 Any of the Parties may act as a Processor by Processing Personal Data on the documented instructions from any of the other Parties, which has determined the purpose and means of Processing and consequently is acting as a Controller. In this case, the Controller and Processor must enter into a data processor contract.

7.8 In the scenarios above the Controllers, whether acting jointly or individually, must identify legal bases to ensure compliance with GDPR, including a condition for Processing special categories Data if this is the case. If the Data are confidential personal data, a basis respecting the common law duty of confidence must also be established.

7.9 The table below presents the five scenarios described above with examples. The reason for highlighting these categories is to provide a focus for those completing DPIAs for their proposed collaborative working initiatives.

| **NHS England and NHS Improvement Collaborative Working**<br><br>**Controllership Scenarios** | | | |
|---|---|---|---|
| | **Controllership type** | **Description** | **Examples** |
| 1. | Joint Controllers – aligned exercise of separate and specific statutory functions | The Parties have separate statutory functions as the basis for conducting activities and Processing Data, but those functions are related, and consequently their exercise is aligned. | Processing to support the following specific functions:<br>• NHS England's functions in respect of the performance assessment of CCGs and giving directions to CCGs; and<br>• NHS Improvement's functions in respect of the oversight and regulation of NHS trusts and Foundation Trusts. |
| 2. | Joint Controllers – general powers and corporate governance arrangements | The Parties collaboratively Process personal data in the exercise of their general powers. | Processing to support the following activities:<br>• The appointment of joint executive positions to the Board and at a senior level<br>• Shared HR service;<br>• Planning for operational management of integrated teams; |

| | | | |
|---|---|---|---|
| | | | • Line management of integrated teams;<br>• The establishment of a shared secretariat for servicing boards and committees. |
| 3. | One Party is a Controller, supported by staff employed by any of the other Parties | One Party alone is responsible for determining the purpose and means of Processing to exercise its own functions and consequently it is the sole Controller. An employee of another of the Parties who assists with the Processing under the guidance, direction or supervision of the sole Controller is acting as an agent of the Party which has the function and which is the Controller. | • Processing to support recruitment, entering into and managing staff contracts.<br>• Processing by teams including members from any of the Parties in support of one of the Parties' functions<br>• Processing of subjects' rights requests by the Corporate Information Governance team under the management of the jointly employed DPO. |
| 4. | Data sharing – with each organisation acting as a separate sole Controller | Personal Data is shared between Parties as separate sole Controllers. | Disclosure by one Party of pseudonymised Personal Data it holds to another Party for purposes determined entirely by the latter. |
| 5. | Processor | One or more of the Parties acts as a Processor for one or more of the other Parties which is/are the Controller(s). The Processing Party does not need to establish a legal basis as it is acting on the instructions of the Controller(s). | One of the Parties acts as Controller responsible for determining the purpose and means of Processing, but the Processing of Data is undertaken by another Party. |

## 8. GDPR – Bases for lawful Processing

8.1 The bases for lawful Processing will depend on the individual purposes and will be assessed on a case by case basis (see clauses 8.5 and 11). Typical examples are given below.

8.2 Where Processing is necessary for the performance of the Parties' respective statutory functions, or exercise of general powers the Parties' basis for lawful Processing may be Article 6(1)(e) of the GDPR – processing is "…necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in [them]…" (scenarios 1 – 3).

8.3 Where Processing is necessary for the performance of one of the Parties' functions, the basis for lawful Processing is that applied by the Party whose functions are being performed, irrespective of whether Processing is undertaken by employees of another Party or Parties (scenario 3).

8.4 Where Processing relates to recruitment or the management of staff contracts, the relevant basis for lawful Processing may be Article 6(1)(b) of the GDPR – processing is "…necessary for the performance of a contract to which the data subject is party…".

8.5 The bases for lawful Processing under GDPR Article 6 and conditions for Processing special category data under Article 9 will be identified and approved in DPIAs conducted prior to implementing functions involving joint Processing and information sharing.

8.6 Where personal data is to be disclosed by one Party to another for the latter's own purposes (scenario 4), the lawful bases and conditions for Processing special category data will be stated in the relevant purpose-specific information sharing agreement.

8.7 Where one or more of the Parties acts as a Processor (scenario 5), it is the responsibility of the Party or Parties that are Controller(s) to identify the lawful bases for Processing.

8.8 The Parties will record details of their Processing as joint or sole Controllers, with their lawful bases and conditions for Processing special category data, in their shared information asset register in accordance with clause 12 below.

8.9 The Parties will publish their bases for lawful Processing and conditions for Processing special category data within their privacy notices.

## 9. Common law duty of confidence

9.1 The Parties agree that when introducing working practices to enable joint working, that any duty of confidence to Data subjects will continue to be respected.

9.2 The Parties will achieve this by addressing confidentiality requirements in their business change and governance processes and in particular through the application of data protection by design and default as described in clause 11.

## 10. Accountability and demonstrating data protection compliance

10.1 The Parties have appointed a single Data Protection Officer (DPO) overseeing a central DPO function for all the Parties. The DPO supported by the DPO function will perform the tasks assigned by Data Protection Law and including:

- reporting to the Parties' accountable officers on their obligations and the state of the Parties' data protection compliance;

- monitoring the Parties' compliance with Data Protection Law;
- providing a central point of contact for consistent advice for the Parties' employees;
- providing a central point of contact for communications with the ICO including:
    - Prior consultation where warranted by conclusions of DPIAs;
    - Managing responses to potential or actual personal data breaches; and
    - Responses regarding complaints or other matters raised.

- operating a process for the central management of responses to personal data requests; and
- operating a single process for the reporting and notification of personal data breaches.

10.2 The Data Protection Officer, supported by the DPO function will oversee the joint activities described in clauses11 – 15, ensuring that the Parties have in place shared or aligned corporate policies and procedures to govern these activities.

10.3 The Parties will appoint a single Senior Information Risk Owner (SIRO), with overall responsibility and accountability for information risk for each of the Parties, and for devising a joint policy for the management of information risk.

10.4 Each of the Parties will continue to appoint a Caldicott guardian.

## 11. Data protection by design and default

11.1 The Parties will collaborate to ensure that data protection by design and default is applied when designing new processes when establishing new joint working practices, mergers of teams etc.

11.2 They will do this by operating a joint *Procedure for IG requirements for New Processes, Services, Information Systems and Assets* and in accordance with this procedure:

- Jointly conducting DPIAs early in the development process, using the agreed DPIA templates, including:
    - assessment of which of the scenarios within the table in clause 7 applies; and
    - establishing the bases for Processing that apply under Articles 6 and 9 of the General Data Protection Regulation (Regulation 9EU) 2016/679) for special categories (if applicable).

- Obtaining approval for completed DPIAs through the established governance process.

The Parties will

- Establish schedules of
    - DPIAs indicating the nature of the Processing activities as joint or sole Controllers
    - Information sharing agreements
    - Data processor agreements

- Where the Parties are to act as joint Controllers (scenarios 1 and 2), or to exercise their individual functions as sole Controllers supported by staff employed by the other Party(ies) (scenario 3) they will:
    - establish or update operational procedures to reflect new working practices and Processing as appropriate; and
    - on approval of the DPIA for the Processing, complete an entry in the DPIA schedule to indicate the nature of the Processing.

- Where the Parties are sharing personal data for the recipient's discrete purposes (scenario 4) they will:
    - enter in to purpose specific data sharing agreements using an agreed standard template; and
    - complete an entry in the schedule of information sharing agreements.

- Where one of the Parties is to act as a data Processor (scenario 5), the contracting Party or Parties will:
    - enter into a binding agreement with them using the agreed standard template;
    - complete an entry in the schedule of data processing agreements;

- ensure that where identifiable personal data is not necessary for the purpose, pseudonymised personal data are used;
- ensure that controls are in place to ensure that access to personal data is restricted to those with a legitimate need for the specified purpose; and
- ensure that privacy information is updated to reflect new working arrangements and joint Processing of to personal data.

## 12. Records of Processing activities

12.1 The Parties will record their information assets on a shared information asset register. This will indicate joint Controller responsibilities where applicable, and include the information required by GDPR Article 30.

12.2 The parties will collaborate to ensure that the entries in their information asset registers are consistent and reflected in their privacy notices as appropriate.

## 13. Privacy information

13.1 The Parties will collaborate to ensure that appropriate privacy information is provided to Data subjects. They will ensure that the information is provided in a concise, transparent, intelligible and easily accessible form.

13.2 Where personal data is not collected from the Data subject, the Parties' online privacy notices will provide the vehicle for informing Data subjects. The Parties will collaborate to ensure that these notices are consistent and reference each other.

13.3 Where the Parties establish systems that collect personal data directly from Data subjects, they will collaborate to make sure that compliant privacy information is presented at the point of contact.

13.4 The privacy information will include information based on the essence of this Agreement presented in clause 6 – as required by GDPR Article 26(2).

## 14. Subjects' rights requests and other requests for personal data

14.1 The Parties are to operate a joint *Procedure for managing personal data requests* for the central management of Data subjects' rights requests, other requests for personal data, and requests for access to records of the deceased – the latter under the Access to Health Records Act 1990 rather than Data Protection Legislation.

14.2 This procedure will cover the responsibilities of the DPO function, IG leads and all staff in contributing to responses to requests for personal data.

14.3 The procedure will enable the DPO function and the Parties' departments to understand and effectively to exercise their respective responsibilities in responding to Data subjects' rights requests and other personal data requests.

## 15. Reporting, management and notification of personal data breaches

15.1 The Parties will operate a shared procedure for the reporting, management and notification of personal data breaches: the *Information security incident reporting procedure.*

15.2 This will involve making a breach reporting portal available to all staff employed by the Parties.

15.3 The DPO will make decisions as to whether to notify personal data breaches to the ICO.

15.4 The DPO will make decisions as to whether to communicate breaches to the Data subjects.

15.4 The DPO function will monitor breach responses to ensure compliance with statutory timescale and other requirements of Data Protection Law.

## 16. Invalidity

16.1 If any provision or part-provision of this Agreement is or becomes invalid or illegal, it shall be deemed modified to the minimum extent necessary to make it valid and legal. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this clause shall not affect the validity of the rest of this Agreement.

16.2 If one Party gives notice to the others of the possibility that any provision or part-provision of this Agreement is invalid or illegal, the Parties shall negotiate in good faith to amend such provision so that, as amended, it is legal and valid, and, to the greatest extent possible, achieves the intended result of the original provision.

## 17 Audit and specific rights

17.1 Each Party will permit the others to audit its compliance with the terms of this Agreement, on at least 14 days' notice. Each Party will provide the others with all reasonably necessary assistance to conduct such audits.

## 18 Liability

18.1 Nothing in this Agreement is intended to limit any Party's liability in respect of the exercise of any of its statutory functions or its obligations to comply with Data Protection Law.

## 19 Dispute Resolution

19.1 The Parties will attempt to resolve any dispute between them in respect of this Agreement in good faith.

19.2 In the event that the Parties are unable to resolve a dispute in accordance with clause 19.1, a Party may at any time serve written notice on the other parties, stating that a dispute exists and setting out the matters in dispute, and the dispute and the dispute shall then be referred to the Chief Executive of NHS England and NHS Improvement for resolution.

## 20 Termination and Variation

20.1 This Agreement will terminate in the event of either of the following:

- On the termination of the Memorandum of Understanding on co-operation; or
- On any Party giving not less than 6 months' notice to the other Parties.

20.2 Termination of this Agreement shall not affect any rights, remedies, obligations or liabilities of the Parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of the Agreement which existed at or before the date of termination.

20.3 No variation of this Agreement will take effect unless it is in writing and signed on behalf of the Parties.

---

## Signatories

Signed by for and on behalf of **NHS ENGLAND**:

_____ Signature

_____ Name (PRINT)

_____ Date

Signed by for and on behalf of **NHS IMPROVEMENT**:

_____ Signature

_____ Name (PRINT)

_____ Date