**Joint Controller Information Sharing Agreement**

**Step Into Health**

**Digital Platform**

**Made on <Date>**

**Between:**

**THE NHS CONFEDERATION**

**and**

**<NHS EMPLOYER>**

Contents

[**1** **INTRODUCTION** 3](#_Toc11422539)

[**2** **DEFINITIONS** 4](#_Toc11422540)

[**3** **PURPOSE OF INFORMATION SHARING** 5](#_Toc11422541)

[**4** **LEGAL BASIS FOR SHARING** 5](#_Toc11422542)

[**5** **ENSURING FAIRNESS TO THE DATA SUBJECT** 6](#_Toc11422543)

[**6** **INFORMATION GOVERNANCE: PERSONNEL** 6](#_Toc11422544)

[**7** **INFORMATION GOVERNANCE: PROTECTION OF PERSONAL INFORMATION** 7](#_Toc11422545)

[**8** **INFORMATION GOVERNANCE: TRANSMISSION OF INFORMATION BETWEEN THE PARTIES** 8](#_Toc11422546)

[**9** **INFORMATION GOVERNANCE: CONFIDENTIALLITY** 8](#_Toc11422547)

[**10** **INFORMATION GOVERNANCE: QUALITY OF INFORMATION** 8](#_Toc11422548)

[**11** **INFORMATION GOVERNANCE: MONITORING, AUDIT AND VARIATION** 8](#_Toc11422549)

[**12** **INFORMATION GOVERNANCE: TERMINATION** 8](#_Toc11422550)

[**13** **INFORMATION GOVERNANCE: RETENTION AND DISPOSAL OF SHARED INFORMATION** 9](#_Toc11422551)

[**14** **INFORMATION GOVERNANCE: COMPLAINTS, ACCESS TO PERSONAL DATA** 9](#_Toc11422552)

[**15** **INFORMATION GOVERNANCE: NOTICES AND DISPUTE RESOLUTION** 9](#_Toc11422553)

# **INTRODUCTION**

This Agreement is made between:

* 1. **The Employer**, legally referred to as **<NHS EMPLOYER>**; and
	2. **The NHS Confederation,** a company limited by guarantee and registered at Companies House in England with company number 04358614 and with registered address Floor 15, Portland House, Bressenden Place, London, SW1E 5BH (“NHS Confederation”). together referred to in this Agreement as the **“Parties”** and each a 3333**“Party”.**
	3. The Parties have agreed to create a digital platform for the Step into Health programme that can be used by three different audiences: employers within the NHS, the candidate from the Armed Forces community and NHS Employers. The digital tool will enable:
* real time and useful analysis of the interactions with candidates and the Step into Health programme for both the local employer and NHS Employers at national level.
* members of the Armed Forces community (candidates) to register their interest in the programme at the point of engagement with the programme.
* NHS organisations to easily record their interactions with candidates and track them through the programme.
	1. The NHS Confederation shall be responsible for designing, building, operating and maintaining the digital platform.
	2. This Agreement covers the sharing of personal data that will be used to support the three different audiences; employers within the NHS, the candidate from the Armed Forces community and NHS Employers.
	3. The purpose of the Data Sharing is set out in greater detail in clause 3 below.
	4. The aim of this Agreement is to remove any potential barriers to and uncertainty about Personal Data sharing at both operational and managerial levels by setting out the requirements each Party must meet.
	5. The Data Protection Act and General Data Protection Regulations state that data sharing should take place in the context of a set of common rules, binding on all the organisations involved, set out in a data sharing arrangement.
	6. This Agreement between the Parties applies only to the Personal Data set out in this Agreement and does not apply to any other data that may be exchanged between the Parties under any other agreements or for other lawful purposes.
	7. This Agreement:
		1. is for the secure and confidential sharing of Personal Data between the Parties in relation to potential and successful candidates.
		2. describes roles and structures to support the exchange of Personal Data between the Parties;
		3. applies to the sharing of Personal Data whatever the medium in which it is held and however it is transmitted;
		4. is designed to ensure that Data Subjects are, where appropriate, informed of the reasons why Personal Data about them may need to be shared and how this sharing will be managed;
		5. applies to the activities of the Parties’ Personnel; and,
		6. describes how complaints from Service Users relating to Personal Data sharing between the Parties will be investigated and resolved.

# **DEFINITIONS**

* 1. The definitions and rules of interpretation in this clause apply in this Agreement:

|  |  |
| --- | --- |
| **“Data Controller”** | shall have the same meaning as set out in the General Data Protection Regulations; |
| **“Data Processor”** | shall have the same meaning as set out in the General Data Protection Regulations; |
| **“Data Protection Law”** | all legislation and regulatory requirements in force from time to time relating to the use of personal data and the privacy of electronic communications, including (i) the Data Protection Act 2018 and any successor UK legislation, as well as (ii) the General Data Protection Regulation ((EU) 2016/679) and any other directly applicable European Union regulation relating to data protection and privacy (for so long as and to the extent that the law of the European Union has legal effect in the UK); |
| **“Data Subject”****“Digital Platform”** | shall have the same meaning as set out in the General Data Protection Regulations;means the website created to deliver the requirements of the candidate monitoring tool;  |
| **“Personal Data”** | shall have the same meaning as in the General Data Protection Regulations; |
| **“Personnel”** | means the Parties’ employees, voluntary staff, consultants, and other contractors and sub-contractors acting on behalf of any Party (whether or not the arrangements with such contractors and sub-contractors are subject to legally binding contracts) and such contractors’ and their sub-contractors’ Personnel; |
| **“Process”** | has the meaning given to it under the General Data Protection Regulations but, for the purposes of this Agreement, it shall include both manual and automatic processing; |
| **“Security Breach”** | means any security breach relating to:(a) Personal Data; or(b) Non-Personal Data reasonably determined by any Party to be sufficiently serious or substantial to give rise to a material risk of litigation by third parties affected by the breach; |
| **“Specified Purpose”** | means the purpose for which the Relevant Information are shared and processed, set out in clause 3 of this Agreement; |
| **“Service Users”** | means anybody registering or having a login to the Digital Platform. |

* 1. Headings are inserted for convenience only and shall not affect the construction or interpretation of this Agreement and, unless otherwise stated, references to clauses and schedules are references to the clauses of and schedules to this Agreement.
	2. Any reference to any enactment or statutory provision shall be deemed to include a reference to the latest version of that enactment and any subordinate legislation made under it and the word ‘including’ shall mean including without limitation or prejudice to the generality of any description, definition, term or phrase preceding that word, and the word ‘include’ and its derivatives shall be construed accordingly.

# **PURPOSE OF INFORMATION SHARING**

* 1. The Specified Purpose of the data sharing initiative is to enable the Parties to have the ability to understand the number and demographics of the candidates engaging with the Step into Health programme and which stage of the journey the candidate is in. Vital to evidencing the success of Step into Health both for the national co-ordination team and local employer.

		1. The Personal Data that will be shared are set out in Schedule 1.

# **LEGAL BASIS FOR SHARING**

* 1. The bases for lawful processing that the Parties apply will depend on the sources of necessity for the respective purposes. Where data is shared between the Parties and subsequently processed, it may be that more than one basis for lawful processing is applicable.
	2. For the purposes of this Agreement, The NHS Confederation and <EMPLOYER> are the Data Controllers. The Parties have identified that it is lawful for the Relevant Information to be shared further to this Agreement.
	3. The collaborative arrangements between the Parties may mean they have a legitimate interest in transmitting personal data between the Parties for administrative purposes which do not relate to the performance of their public tasks or other purposes, in which case Article 6(1)(f) of the GDPR may apply – processing is “…necessary for the purposes of the legitimate interests pursued by the controller or a third party…”.

# **ENSURING FAIRNESS TO THE DATA SUBJECT**

* 1. In addition to having a lawful basis for sharing information, the General Data Protection Regulations requires that the sharing must be fair. In order to achieve fairness to the Data Subjects, the Parties will ensure that all candidates are aware that their information will be shared by both the NHS Confederation and the Employers.
	2. The Parties will collaborate to ensure that appropriate privacy information is provided to subjects. They will ensure that the information is provided in a concise, transparent, intelligible and easily accessible form.
	3. Where data is not collected from the subject, the Parties’ online privacy notices will provide the vehicle for informing subjects. The parties will collaborate to ensure that these notices are consistent and reference each other.
	4. Where the Parties establish systems that collect personal data directly from subjects, they will collaborate to make sure that compliant privacy information is presented at the point of contact.
	5. This Agreement helps to ensure fairness by ensuring there are parameters to the sharing of the information and documenting the information governance procedures that the Parties have in place.

# **INFORMATION GOVERNANCE: PERSONNEL**

* 1. Each Party shall take reasonable steps to ensure the reliability of any Personnel who have access to the Personal Data including reasonable background checks.
	2. Each Party shall provide evidence (further to any reasonable request) that all Personnel that have any access to the Personal Data whatsoever are adequately and appropriately trained to comply with their responsibilities under the General Data Protection Regulations and this Agreement.
	3. Each Party shall ensure that:
		1. only those employees involved in delivery of the Agreement use or have access to the personal data; and
		2. that such access is granted on a strict Need to Know basis
		3. and shall implement appropriate access controls to ensure this requirement is satisfied and audited.
	4. Specific limitations on the Personnel who may have access to the Information are set out in the Schedule 1.

# **INFORMATION GOVERNANCE: PROTECTION OF PERSONAL INFORMATION**

* 1. At all times, the Parties shall have regard to the requirements of the General Data Protection Regulations and the rights of Data Subjects.
	2. Processing of any Personal Data shall be to the minimum extent necessary and on a Need to Know basis.
	3. If either Party:
		1. becomes aware of any unauthorised or unlawful processing of any personal data or that any personal data is lost or destroyed or has become damaged, corrupted or unusable; or
		2. becomes aware of any Security Breach;
		3. in respect of the personal data it shall promptly notify the other Party. The Parties shall fully cooperate with one another to remedy the issue as soon as reasonably practicable.
	4. Each Party shall act in accordance with the Principles and in particular shall implement and maintain appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected. In particular, each Data Processor shall:
		1. ensure that only Personnel authorised under this Agreement have access to the Personal Data;
		2. ensure that the Personal Data is kept secure and shall use all reasonable security practices and systems applicable to the use of the Personal Data to prevent and to take prompt and proper remedial action against, unauthorised access, copying, modification, storage, reproduction, display or distribution, of the Personal Data;
		3. if any processing of the Personal Data is done outside the EEA, ensure that the country has an adequacy decision or appropriate safeguards are in place.
		4. if requested, provide a written description of the technical and organisational methods and security measures employed in protecting Personal Data.
	5. Specific requirements as to information security are set out in Schedule 1.
	6. The Parties’ Single Point of Contacts (SPoC’s) set out in Clause 15 will be the persons who, in the first instance, will have oversight of third party security measures.

# **INFORMATION GOVERNANCE: TRANSMISSION OF INFORMATION BETWEEN THE PARTIES**

* 1. Transfer of Personal Data between the Parties shall be done through the digital platform.
	2. Any other special measures relating to security of transfer are specified in the Schedule 1.

# **INFORMATION GOVERNANCE: CONFIDENTIALLITY**

* 1. The Parties agree to treat all Personal Data as confidential and imparted in confidence and shall safeguard it accordingly. The employing Parties shall ensure that its Personnel operate under a duty of confidentiality.
	2. Respect for the privacy of individuals and the other Party will be afforded at all stages of carrying out the Specified Purpose.

# **INFORMATION GOVERNANCE: QUALITY OF INFORMATION**

* 1. The Parties will take steps to ensure the quality of the Personal Data and to comply with the obligations in Article 5(1) of the General Data Protection Regulations.

# **INFORMATION GOVERNANCE: MONITORING, AUDIT AND VARIATION**

* 1. The Parties shall appoint one person from each Party whose role will be to monitor this Agreement and any complaints and concerns received regarding its implementation. Unless agreed otherwise, this will be the SPoC named in Clause 15.
	2. The Parties together shall review this Agreementsix months after the first date upon which it is signed and thereafter no less frequently than twelve monthly.
	3. The review shall address the following issues:
		1. The operational effectiveness of the Agreement;
		2. Any changes that may be required to the Agreement;
		3. Any incidents of non-compliance or other such issues;
		4. Any other matters the Parties wish to discuss.
	4. Any changes or modifications to this Agreement that may be deemed necessary from time to time by the Parties, or requested by either Party, shall only be valid once issued in writing and signed by authorised representatives of both Parties.
	5. Once the Specified Purpose has been achieved or where there is a change in circumstances which necessitates an urgent review, this Agreement shall again be reviewed promptly by the Parties.
	6. The Parties may together or individually audit the quality of information shared under this Agreement and the efficacy of the Agreement. The outcomes of such audit will be shared with the other Party.

# **INFORMATION GOVERNANCE: TERMINATION**

* 1. This agreement will remain in place for the duration that The NHS Confederation has the responsibility for operating and maintaining the digital platform.

# **INFORMATION GOVERNANCE: RETENTION AND DISPOSAL OF SHARED INFORMATION**

* 1. Each Party will have a data -retention policy, for the Personal Data, that is included in each published Privacy Policy.
	2. The Parties shall ensure that, when no longer required, electronic storage media used to hold or process Personal Data are destroyed or overwritten to current policy requirements.

# **INFORMATION GOVERNANCE: COMPLAINTS, ACCESS TO PERSONAL DATA**

* 1. The Parties will use their own procedures to respond to any request made under Data Protection Law or the General Data Protection Regulations made by persons who wish to access copies of information held about them (“**Subject Access Requests**”).
	2. Complaints about information sharing shall be routed through the Data Controller’s complaints procedure and reported to its SPoC under this Agreement.
	3. The Parties shall use all reasonable endeavours to work together to resolve any dispute or complaint arising under this Agreement or any data processing carried out further to it.

Each Party shall consult the other regarding commercial, data protection or other confidentiality issues in relation to the information requested.

# **INFORMATION GOVERNANCE: NOTICES AND DISPUTE RESOLUTION**

* 1. Each Party shall nominate a SPoC who will be the first point of contact for the management of this Agreement. For each organisation, the SpoC is:

|  |  |  |
| --- | --- | --- |
| **Party** | **Single Point of Contact (SpoC)** | **Contact details** |
| NHS Confederation | Gemma Wright |  |
| Employer 1 |  |  |
| Employer 2 |  |  |
| Employer 3 |  |  |
| Employer 4 |  |  |

**SIGNATORIES**

**SIGNED** on and on behalf of The NHS Confederation

Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name (PRINT) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SIGNED** on and on behalf of **<EMPLOYER>**

Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name (PRINT) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SCHEDULE 1**

| **Clause** | **Special Issues** | **Details** |
| --- | --- | --- |
| 3 | Personal Data to be shared under this Agreement | 1. Name;
2. Contact Details;
3. Date of Birth;
4. Armed Forces Community Description;
5. Service Number;
6. Rank;
7. Date of leaving/available;
8. Current location/location of interest;
9. Job Type;
10. Roles/Areas of interest;
11. Source of referral;
12. Contacts and narratives.
 |
| 6 | Limitations on Personnel who have access to the Personal Data | * Supervisory checks should be undertaken (frequency depends on activity) to ensure that Personnel are working in accordance with agreed processes, policies and procedures in line with best practice.
* Where necessary, detailed written instructions providing a step by step guide for the distribution of Personal Data should be produced for staff implementing the procedure
 |
| 7 | Security requirements for the Personal Data | * Only authorised Personnel will have access to any SharePoint sites containing Personal Data.
* Personnel with access to any Digital Platform containing Personal Data will be re-validated every 3 months.
 |
| 8 | Transmission of Information | * Any Personal Data transferred by Spreadsheets shall be password protected.
* Personal Data held on the Digital Platform sites may only be accessed by authorised Personnel
 |