

**DATED**

**14<sup>TH</sup> OCTOBER 2022**

---

**(1) HEALTH AND CARE PROFESSIONS COUNCIL**

**and**

**(2) HEALTH EDUCATION ENGLAND**

---

**DATA SHARING AGREEMENT**

---



**BDB PITMANS**

**Registered Office**

One Bartholomew Close  
London  
EC1A 7BL  
DX 339401 London Wall

50/60 Station Road  
Cambridge  
CB1 2JH  
DX 339601 Cambridge 24

The Anchorage  
34 Bridge Street  
Reading, RG1 2LU  
DX 146420 Reading 21

Grosvenor House  
Grosvenor Square  
Southampton, SO15 2BE  
DX 38516 Southampton 3

**T** +44 (0)345 222 9222

**W** [www.bdbpitmans.com](http://www.bdbpitmans.com)



## TABLE OF CONTENTS

1	Interpretation	1
2	Purpose	5
3	Shared Personal Data	6
4	Lawful, fair and transparent processing; Joint Controller responsibilities	7
5	Data quality	7
6	Data Subjects' Rights	8
7	Data retention and deletion	8
8	Transfers	9
9	Security and training	9
10	Personal data breaches and reporting procedures	10
11	Confidentiality	10
12	Review and termination of agreement	11
13	Resolution of disputes with data subjects or the Information Commissioner	12
14	Freedom of Information	12
15	Warranties	13
16	Indemnity	14
17	Limitation of liability	15
18	Third party rights	16
19	Variation	16
20	Waiver	16

21	Severance	16
22	Changes to the applicable law	17
23	No partnership or agency	17
24	Entire agreement	17
25	Further assurance	17
26	Force majeure	17
27	Notice	18
28	Governing law	18
29	Jurisdiction	18
	SCHEDULE 1	19
	NOT USED	19
	SCHEDULE 2	20
	Further Detail on Shared Personal Data and Access and Processing Restrictions	20
	NOT USED	24
	SCHEDULE 4	25
	NOT USED	25
	SCHEDULE 5	26
	NOT USED	26
	SCHEDULE 6	27
	Appropriate Technical and Organisational Security Measures	27
	SCHEDULE 7	28
	NOT USED	28
	SCHEDULE 8	29
	NOT USED	29
	SCHEDULE 9	30
	Lawful Bases (and Conditions or Exceptions for processing of any Special Categories of Personal Data and Criminal Offence Data) and Legal Power for Data Sharing	30
	SCHEDULE 10	31
	NOT USED	31

**THIS AGREEMENT** is dated 14 October 2022

## PARTIES

- (1) Health and Care Professions Council whose registered office is at Park House, 184-186 Kennington Park Road, London SE11 4BU (**HCPC**)
- (2) Health Education England whose registered office is at 4, Stewart House, 32 Russell Square, London WC1B 5DN (**HEE**)

## BACKGROUND

- (A) The parties have determined that they are Independent Controllers in relation to the Shared Personal Data and accordingly this agreement sets out the arrangements between them for the purposes of the Data Protection Legislation.
- (B) HCPC agrees to share the Shared Personal Data with the HEE on the terms set out in this agreement.
- (C) HEE agrees to use the Shared Personal Data on the terms set out in this agreement.
- (D) This is a free-standing agreement that does not incorporate any commercial terms established by the parties under separate commercial arrangements.

## AGREED TERMS

### 1 Interpretation

The following definitions and rules of interpretation apply in this agreement.

#### 1.1 Definitions:

<b>Agreed Purpose</b>	has the meaning given to it in clause 2 of this agreement.
<b>Business Day</b>	a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business.
<b>Commencement Date</b>	14 <sup>th</sup> October 2022
<b>Commercially Sensitive Information</b>	the information listed in Schedule 10 comprising the information of a commercially sensitive nature relating to a party, its intellectual property rights or its business or which that party has indicated to the other party that, if disclosed by the other party pursuant to a Request for Information, would cause significant commercial disadvantage or material financial loss.
<b>Confidential Information</b>	means all confidential information (however recorded or preserved) disclosed by a party or its Representatives to the other

party and that party's Representatives in connection with this agreement, including but not limited to:

- a) any information that would be regarded as confidential by a reasonable business person relating to: (i) the business, affairs, customers, suppliers or plans of the disclosing party; and (ii) the operations, processes, product information, know-how, designs, trade secrets or software of the disclosing party;
- b) any information developed by the parties in the course of carrying out this agreement;
- c) Personal Data;
- d) any Commercially Sensitive Information.

**Criminal Offence Data** means Personal Data relating to criminal convictions and offences or related security measures to be read in accordance with section 11(2) of the Data Protection Act 2018.

**Data Protection Legislation** all applicable data protection and privacy legislation in force from time to time in the UK including the UK GDPR; the Data Protection Act 2018 (DPA 2018) (and regulations made thereunder) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications), and the guidance and codes of practice issued by the Information Commissioner or other relevant data protection or supervisory authority and applicable to a party.

**Deletion Procedure** has the meaning given to it in clause 7.3 of and Schedule 5 to this agreement.

**EIRs** the Environmental Information Regulations 2004 (SI 2004/3391) together with any guidance and/or codes of practice issued by the Information Commissioner or relevant government department in relation to such regulations.

**FOIA** the Freedom of Information Act 2000 together with any guidance and/or codes of practice issued by the Information Commissioner or relevant government department in relation to such legislation.

**Force Majeure Event** means any event beyond the reasonable control of the Party in question to include, without limitation:  
  
(a) war including civil war (whether declared or undeclared), riot, civil commotion or armed conflict materially affecting either Party's ability to perform its obligations under this Contract;  
  
(b) acts of terrorism;

(c) flood, storm or other natural disasters;

(d) fire;

(e) unavailability of public utilities and/or access to transport networks to the extent no diligent supplier could reasonably have planned for such unavailability as part of its business continuity planning;

(f) government requisition or impoundment to the extent such requisition or impoundment does not result from any failure by the Supplier to comply with any relevant regulations, laws or procedures (including such laws or regulations relating to the payment of any duties or taxes) and subject to the Supplier having used all reasonable legal means to resist such requisition or impoundment;

(g) compliance with any local law or governmental order, rule, regulation or direction applicable outside of England and Wales that could not have been reasonably foreseen;

(h) industrial action which affects the ability of the Supplier to provide the Services, but which is not confined to the workforce of the Supplier or the workforce of any Sub-contractor of the Supplier; and

(i) a failure in the Supplier's and/or Authority's supply chain to the extent that such failure is due to any event suffered by a member of such supply chain, which would also qualify as a Force Majeure Event in accordance with this definition had it been suffered by one of the Parties; but excluding, for the avoidance of doubt, the withdrawal of the United Kingdom from the European Union and any related circumstances, events, changes or requirements;

<b>Information</b>	has the meaning given under section 84 of FOIA.
<b>Joint Controller</b>	means where two or more Controllers jointly determine the purposes and means of processing, as referred to in Article 26 of the UK GDPR.
<b>Personal Data Breach</b>	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data.
<b>Representatives</b>	means, in relation to a party, its employees, officers, contractors, subcontractors, representatives and advisors.
<b>Request for Information</b>	a request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the EIRs.

<b>Shared Personal Data</b>	the Personal Data to be shared between the parties under clause 3 of this agreement.
<b>Special Categories of Personal Data</b>	the categories of Personal Data set out in Article 9(1) of the UK GDPR.
<b>Subject Rights Request</b>	the exercise by a Data Subject of his or her rights under the Data Protection Legislation.
<b>Term</b>	. Until terminated in accordance with Clause 12.
<b>UK GDPR</b>	has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

- 1.2 **Controller, Processor, Data Subject, Information Commissioner and Personal Data, Processing and appropriate technical and organisational** measures shall have the meanings given to them in the Data Protection Legislation.
- 1.3 **Public Authority** shall have the meaning as set out in section 7 of the DPA 2018.
- 1.4 Clause, Schedule and paragraph headings shall not affect the interpretation of this agreement.
- 1.5 The Schedules form part of this agreement and shall have effect as if set out in full in the body of this agreement. Any reference to this agreement includes the Schedules.
- 1.6 Unless the context otherwise, requires, words in the singular shall include the plural and in the plural shall include the singular.
- 1.7 A reference to a legislation or legislative provision shall include all subordinate legislation made from time to time under that legislation or legislative provision.
- 1.8 References to clauses and Schedules are to the clauses of and Schedules to this agreement and references to paragraphs are to paragraphs of the relevant Schedule.
- 1.9 Any words following the terms **including, include, in particular** or **for example** or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding these terms.
- 1.10 In the case of any ambiguity between any provision contained in the body of this agreement and any provision contained in the Schedules or appendices, the provision in the body of this agreement shall take precedence.
- 1.11 A reference to **writing** or **written** includes email.
- 1.12 Unless the context otherwise requires the reference to one gender shall include a reference to the other genders.



## 2 Purpose

2.1 This agreement sets out the framework for the sharing of **Personal Data** when one **Controller** (the **Data Discloser**) discloses Personal Data to another **Controller** (the **Data Receiver**). It defines the principles and procedures that the parties shall adhere to and the responsibilities the parties owe to each other.

2.2 Each party is a Public Authority and considers this data sharing initiative necessary as:

2.2.1 HEE needs access to the Shared Personal Data in order to undertake analysis of trends in the workforce of allied health professional ('AHPs') that HCPC regulates, to develop better workforce planning and modelling, and monitoring progress against HEE's national mandate of growing the AHP workforce (including monitoring progress against the national target for AHPs returning to practice). HEE needs to do those things in order to carry out its public tasks to ensure the adequate supply of qualified individuals to meet NHS England workforce needs pursuant to HEE's functions under the Care Act 2014. Section 97 of that Act requires HEE to secure that there is an effective system for the planning and delivery of education and training to persons who are employed, or who are considering becoming employed, in an activity which involves or is connected with the provision of services as part of the health service in England. Section 98 of the Care Act 2014 requires HEE to exercise its functions with a view to ensuring that a sufficient number of persons with the skills and training to work as health care workers for the purposes of the health service is available to do so throughout England;

2.2.2 The Health Professions Order 2001 (the '2001 Order') states that the functions of HCPC include establishing and maintaining standards of education and training for members of the professions that it regulates (Article 3(2) of the 2001 Order) and to establish and maintain a register of members of those professions (Article 5(1) of the 2001 Order). HCPC has a duty pursuant to Article 3(5)(b) of the 2001 Order to co-operate in the exercise of its functions, where appropriate, with persons concerned with the employment or education of registrants or the management of health or education services. HEE falls within that category of persons and has requested that HCPC share the Shared Personal Data for the Agreed Purposes. The Shared Personal Data is data that HCPC holds and processes in the exercise of its functions, and for the reasons outlined below HCPC considers that sharing the data is an appropriate form of co-operation with HEE in the exercise of HCPC's functions. The data sharing is therefore necessary in order to fulfil HCPC's statutory duty to co-operate in such a situation.

2.2.3 Article 3(4) of the 2001 Order establishes HCPC's over-arching objective in exercising its functions as "the protection of the public". This includes an objective to "protect, promote and maintain the health, safety and wellbeing of the public" (Article 3(4A)(a) of the 2001 Order). Helping to ensure safe staffing levels of AHPs is necessary for this objective to be achieved. The impact on patient safety from inadequate staffing has been well documented. The National Health Service faces unprecedented pressures following the demands placed on it during the COVID 19 pandemic, and if HCPC is to continue to protect, promote and maintain the health, safety and wellbeing of the public through the exercise of its functions, HCPC needs

to support initiatives aimed at achieving safe staffing levels of AHPs within the NHS. Health Education England is the organisation that ensures NHS England has the right number of AHPs it needs to deliver safe and effective healthcare. HEE also ensures that those AHPs receive appropriate education and training, which the AHPs need in order to meet the standards established by HCPC. The proposed data sharing is a proportionate means of pursuing the statutory objective in Article 3(4) of the 2001 Order and fulfilling HCPC's statutory duty to co-operate with HEE in the exercise of HCPC's functions. The data sharing is therefore necessary for the exercise of official authority vested in HCPC.

2.3 The parties agree that HEE shall only process Shared Personal Data, as described in clause 3.1 for the following purposes:

2.3.1 to enable HEE to conduct statistical analysis of trends in the workforce of AHPs, to undertake workforce planning and modelling at an aggregate level, and to monitor progress against HEE's national mandate of growing the AHP workforce (including monitoring progress against the national target for AHPs returning to practice);

2.3.2 to match individual records in the Shared Personal Data against other datasets already held by HEE, and to update data held by HEE, but in each case only for the purposes outlined at clause 2.3.1 above;

2.3.3 not to make any decisions about individual data subjects; and

2.3.4 not to disclose the Shared Personal Data to any third party except to the extent necessary for the purposes outlined at clause 2.3.1 above,

The parties shall not process Shared Personal Data in a way that is incompatible with the purposes described in this clause (together the **Agreed Purpose**).

2.4 Each party shall appoint a single point of contact (**SPoC**) who will work together to reach an agreement with regards to any issues arising from the data sharing and to actively improve the effectiveness of the data sharing initiative. The points of contact for each of the parties are:

2.4.1 Kate Aitken, Senior Project Manager, HEE National Data Service

2.4.2 Geoff Kirk, Head of IT & Digital Transformation, HCPC

### **3 Shared Personal Data**

3.1 The types of Personal Data that will be shared between the parties during the Term of this agreement are set out in Schedule 2.

3.2 Special Categories of Personal Data will not be shared between the parties.

3.3 Criminal Offence Data will not be shared between the parties

3.4 Further detail on the Shared Personal Data as described in clause 3.1 is set out in Schedule 2 together with any access and processing restrictions as agreed and established by the parties.

3.5 The Shared Personal Data must not be irrelevant or excessive with regard to the Agreed Purpose.

#### **4 Lawful, fair and transparent processing; Joint Controller responsibilities**

4.1 Each party shall ensure that it processes the Shared Personal Data fairly and lawfully in accordance with clause 4.2 during the Term of this agreement.

4.2 Each party shall ensure that it has legitimate grounds under the Data Protection Legislation for the processing of Shared Personal Data. Where the legal basis is consent there must be written evidence of that consent, which is set out in Schedule 3 to this agreement.

4.3 The lawful bases (and conditions or exceptions for processing of any Special Categories of Personal Data or Criminal Offence Data) and the legal power for data sharing are set out in Schedule 9.

4.4 The Data Discloser shall, in respect of Shared Personal Data, ensure that it provides clear and sufficient information to the Data Subjects, in accordance with the Data Protection Legislation, of the purposes for which it will process their personal data, the legal basis for those purposes and such other information as is required by Article 13 of the UK GDPR including:

4.4.1 if Shared Personal Data will be transferred to a third party, that fact and sufficient information about that transfer and the purpose of that transfer to enable the Data Subject to understand the purpose and risks of that transfer; and

4.4.2 if Shared Personal Data will be transferred outside the UK. pursuant to clause 8.4 of this agreement, that fact and sufficient information about that transfer, the purpose of that transfer and the safeguards put in place by the Controller to enable the Data Subject to understand the purpose and risks of that transfer.

4.4.3 The Data Receiver undertakes to inform the Data Subjects, in accordance with the Data Protection Legislation, of the purposes for which it will process their personal data, the legal basis for those purposes and such other information as is required by Article 14 of the UK GDPR including:

4.4.4 if Shared Personal Data will be transferred to a third party, that fact and sufficient information about that transfer and the purpose of that transfer to enable the Data Subject to understand the purpose and risks of that transfer; and

4.4.5 if Shared Personal Data will be transferred outside the UK. pursuant to clause 8.4 of this agreement, that fact and sufficient information about that transfer, the purpose of that transfer and the safeguards put in place by the Controller to enable the Data Subject to understand the purpose and risks of that transfer.

#### **5 Data quality**

5.1 The parties have developed a reliable means of converting Shared Personal Data to ensure compatibility with each party's respective datasets as set out in Schedule 4.

5.2 The Data Discloser shall ensure that before the Commencement Date, Shared Personal Data is an accurate reflection of the data it holds and that it has appropriate internal procedures in place for the Data Receiver to sample Shared Personal Data before the Commencement Date and it will update the same if required before transferring the Shared Personal Data.

5.3 Shared Personal Data must be limited to the Personal Data described in clause 3.1 [and Schedule 2] of this agreement.

## **6 Data Subjects' Rights**

6.1 The parties each agree to provide such assistance as is reasonably required to enable the other party to comply with Subject Rights Requests within the time limits imposed by the Data Protection Legislation.

6.2 The SPoC for each party is responsible for maintaining a record of Subject Rights Requests, the decisions made and any information that was exchanged. Records must include copies of the request for information, details of the data accessed and shared and where relevant, notes of any meeting, correspondence or phone calls relating to the request. The SPoC for each party is detailed in clause 2.4.

## **7 Data retention and deletion**

7.1 The Data Receiver shall not retain or process Shared Personal Data for longer than is necessary to carry out the Agreed Purpose.

7.2 Notwithstanding clause 7.1, parties shall continue to retain Shared Personal Data in accordance with any statutory or regulatory retention periods applicable to them. The parties may put in place common rules for the retention and deletion of Shared Personal Data which shall be set out in Schedule 5.

7.3 The Data Receiver shall ensure that any Shared Personal Data is returned to the Data Discloser or destroyed in accordance with appropriate best practices and ICO guidance:

7.3.1 on termination of the agreement;

7.3.2 on expiry of the Term of the agreement; or

7.3.3 once processing of the Shared Personal Data is no longer necessary for the purposes it was originally shared for, as set out in clause 2.3

(whichever occurs first).

7.4 Following the deletion of Shared Personal Data in accordance with clause 7.3, the Data Receiver shall notify the Data Discloser that the Shared Personal Data in question has been deleted in accordance with appropriate best practices and ICO guidance..

## **8 Transfers**

8.1 For the purposes of this clause, transfers of Personal Data shall mean any sharing of the Shared Personal Data by the Data Receiver with a third party, and shall include, but is not limited to, the following:

8.1.1 subcontracting the processing of Shared Personal Data; and

8.1.2 granting a third party Controller access to the Shared Personal Data.

8.2 The Data Receiver may not, without the Data Discloser's prior written consent:

8.2.1 subcontract the processing of Shared Personal Data;

8.2.2 grant a third party Controller access to the Shared Personal Data; or

8.2.3 transfer the Shared Personal Data outside the UK.

8.3 If the Data Receiver appoints a third party Processor to process the Shared Personal Data it shall comply with Article 28 of the UK GDPR and shall remain liable to the Data Discloser for the acts and omissions of the Processor.

8.4 The Data Receiver may not transfer Shared Personal Data to a third party located outside the UK unless it:

8.4.1 complies with the provisions of Article 26 of the UK GDPR (in the event the third party is a Joint Controller); and

8.4.2 ensures that (i) the transfer is to a country approved under the Data Protection Legislation as providing adequate protection; (ii) there are appropriate safeguards or binding corporate rules in place pursuant to the Data Protection Legislation; or (iii) the transferor otherwise complies with its obligations under the applicable Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; or one of the derogations for specific situations in the Data Protection Legislation applies to the transfer.

## **9 Security and training**

9.1 The Data Discloser shall only provide the Shared Personal Data to the Data Receiver by using secure methods as agreed and set out in Schedule 6.

9.2 The parties undertake to have in place throughout the Term appropriate technical and organisational security measures to:

9.2.1 prevent:

(a) unauthorised or unlawful processing of the Shared Personal Data; and

(b) the accidental loss or destruction of, or damage to, the Shared Personal Data;

- 9.2.2 ensure a level of security appropriate to:
- (a) the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage; and
  - (b) the nature of the Shared Personal Data to be protected.

9.3 The level of technical and organisational measures agreed by the parties as appropriate as at the Commencement Date having regard to the state of technological development and the cost of implementing those measures is set out in Schedule 6. The parties shall keep those security measures under review and shall carry out those updates as they agree are appropriate throughout the Term.

9.4 It is the responsibility of each party to ensure that its staff members are appropriately trained to handle and process the Shared Personal Data in accordance with the technical and organisational security measures set out in Schedule 6 together with any other applicable laws and guidance and that those staff members have entered into confidentiality agreements relating to the processing of Personal Data.

9.5 The level, content and regularity of training referred to in clause 9.4 shall be proportionate to the staff members' role, responsibility and frequency with respect to their handling and processing of the Shared Personal Data.

## **10 Personal data breaches and reporting procedures**

10.1 The parties shall each comply with its obligation to report a Personal Data Breach to the Information Commissioner and (where applicable) Data Subjects under Article 33 of the UK GDPR and shall each inform the other party of any Personal Data Breach irrespective of whether there is a requirement to notify the Information Commissioner or Data Subject(s).

10.2 The parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any Personal Data Breach in an expeditious and compliant manner.

## **11 Confidentiality**

11.1 Subject to clause 11.2, each party shall keep the other party's Confidential Information confidential and shall not:

11.1.1 use such Confidential Information except for the purpose of performing its rights and obligations under or in connection with this agreement; or

11.1.2 disclose such Confidential Information in whole or in part to any third party, except as expressly permitted by this clause 11.

11.2 The obligation to maintain confidentiality of Confidential Information does not apply to any Confidential information:

11.2.1 which the other party confirms in writing is not required to be treated as Confidential Information;

- 11.2.2 which is obtained from a third party who is lawfully authorised to disclose such information without any obligation of confidentiality;
  - 11.2.3 which a party is required to disclose by judicial, administrative, governmental or regulatory process in connection with any action, suit, proceedings or claim or otherwise by applicable law, including the FOIA or the EIRs;
  - 11.2.4 which is in or enters the public domain other than through any disclosure prohibited by this agreement;
  - 11.2.5 which a party can demonstrate was lawfully in its possession prior to receipt from the other party; or
  - 11.2.6 which is disclosed by the Data Discloser on a confidential basis to any central government or regulatory body.
- 11.3 A party may disclose the other party's Confidential information to those of its Representatives who need to know such Confidential Information for the purposes of performing or advising on the party's obligations under this agreement, provided that:
- 11.3.1 it informs such Representatives of the confidential nature of the Confidential Information before disclosure; and
  - 11.3.2 it procures that its Representatives shall, in relation to any Confidential Information disclosed to them, comply with the obligations set out in this clause as if they were a party to this agreement,
  - 11.3.3 and at all times, it is liable for the failure of any Representatives to comply with the obligations set out in this clause 11.3.
- 11.4 The provisions of this clause 11 shall survive for a period of 10 years from the date of expiry or termination of this agreement.

## **12 Review and termination of agreement**

- 12.1 Either party may terminate this agreement by giving the other no less than 3 months' written notice.
- 12.2 Parties shall review the effectiveness of this data sharing initiative every 12 months, having consideration to the aims and purposes set out in clause 2.2 and clause 2.3. The parties shall continue, amend or terminate the agreement depending on the outcome of this review.
- 12.3 The review of the effectiveness of the data sharing initiative will involve:
- 12.3.1 assessing whether the purposes for which the Shared Personal Data is being processed are still the ones listed in clause 2.3 of and Schedule 1 to this agreement;
  - 12.3.2 assessing whether the Shared Personal Data is still as listed in clause 3 of this agreement;

- 12.3.3 assessing whether the parties can continue to rely on a lawful basis or a condition or exception under Data Protection Legislation to lawfully share the Shared Personal Data;
  - 12.3.4 assessing whether the legal framework governing data quality, retention, and Data Subjects' rights is being complied with; and
  - 12.3.5 assessing whether Personal Data Breaches involving the Shared Personal Data have been handled in accordance with this agreement and the applicable legal framework.
- 12.4 Each party reserves its rights to inspect the other party's arrangements for the processing of Shared Personal Data and to terminate the agreement where it considers that the other party is not processing the Shared Personal Data in accordance with this agreement.
- 12.5 The Data Discloser may terminate this agreement with immediate effect by the service of written notice to the Data Receiver if the Data Receiver is in breach of any material obligation under this agreement provided that if the breach is capable of remedy, the Data Discloser may only terminate this agreement if the Data Receiver has failed to remedy such breach within 28 days of receipt of notice from the Data Discloser to do so. For the purposes of this clause 12.5, a material breach incapable of remedy shall include, but not be limited to, a Personal Data Breach.

### **13 Resolution of disputes with data subjects or the Information Commissioner**

- 13.1 In the event of a dispute or claim brought by a Data Subject or the Information Commissioner concerning the processing of Shared Personal Data against either or both parties, the parties will inform each other about any such disputes or claims, and will co-operate with a view to settling them amicably in a timely fashion.
- 13.2 The parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the Information Commissioner. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.
- 13.3 Each party shall abide by a decision of a competent court in the UK or of the Information Commissioner.

### **14 Freedom of Information**

- 14.1 Each party acknowledges that the other party is subject to the requirements of the FOIA and the EIRs. In the event that a party (**Party A**) receives a Request for Information, the other party (**Party B**) shall:
- 14.1.1 provide all necessary assistance and cooperation as reasonably requested by Party A to enable Party A to comply with its obligations under the FOIA and EIRs;



- 14.1.2 transfer to Party A all Requests for Information relating to this agreement that it receives as soon as practicable and in any event within 2 Business Days of receipt;
  - 14.1.3 provide Party A with a copy of all Information belonging to Party A requested in the Request For Information which is in its possession or control in the form that Party A requires within 5 Business Days (or such other period as Party A may reasonably specify) of Party A's request for such Information; and
  - 14.1.4 not respond directly to a Request For Information unless authorised in writing to do so by Party A.
- 14.2 Party B acknowledges that Party A may be required under the FOIA and EIRs to disclose Information (including Commercially Sensitive Information) without consulting or obtaining consent from Party B. Party A shall take reasonable steps to notify Party B of a Request For Information (in accordance with the Cabinet Office's Freedom of Information Code of Practice issued under section 45 of the FOIA) to the extent that it is permissible and reasonably practical for it to do so but (notwithstanding any other provision in this agreement) Party A shall be responsible for determining in its absolute discretion whether any Commercially Sensitive Information and/or any other information is exempt from disclosure in accordance with the FOIA and/or the EIRs.
- 14.3 Notwithstanding any other term of this agreement, Party B consents to the publication of this agreement in its entirety (including variations), subject only to the redaction of information that is exempt from disclosure in accordance with the provisions of the FOIA and EIRs.
- 14.4 Party A shall, prior to publication, consult with Party B on the manner and format of publication and to inform its decision regarding any redactions but shall have the final decisions in its absolute discretion. Party B shall assist and co-operate with Party A to enable Party A to publish this agreement.

## **15 Warranties**

- 15.1 Each party warrants and undertakes that it will:
- 15.1.1 process the Shared Personal Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments that apply to its Personal Data processing operations;
  - 15.1.2 make available on request to the Data Subjects who are third party beneficiaries a copy of this agreement, unless the agreement contains Confidential Information in which case an extract can be provided;
  - 15.1.3 respond within a reasonable time and as far as reasonably possible to enquiries from the Information Commissioner in relation to the Shared Personal Data;
  - 15.1.4 respond to Subject Rights Requests in accordance with the Data Protection Legislation;

- 15.1.5 where applicable, pay the appropriate fees with the Information Commissioner to process all Shared Personal Data for the Agreed Purpose; and
- 15.1.6 take all appropriate steps to ensure compliance with the security measures set out in clause 9 above.
- 15.2 The Data Discloser warrants and undertakes that it is entitled to provide the Shared Personal Data to the Data Receiver and it will ensure that the Shared Personal Data is accurate.
- 15.3 The Data Receiver warrants and undertakes that it will not disclose or transfer the Shared Personal Data to a third party Controller located outside the UK unless it complies with the obligations set out in clauses 8.2-8.4above.
- 15.4 Except as expressly stated in this agreement, all warranties, conditions and terms, whether express or implied by statute, common law or otherwise are hereby excluded to the extent permitted by law.

## **16 Indemnity**

16.1 **General Indemnity.** The Data Discloser and Data Receiver undertake to indemnify each other and hold each other harmless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of the provisions of this agreement, except to the extent that any such liability is excluded under clause 17.2.

### **16.2 UK GDPR Indemnity.**

16.2.1 Each Indemnifying Party undertakes to indemnify each Indemnified Party and hold the Indemnified Party/ies harmless from and against any Loss suffered by the Indemnified Party/ies as a result of joint liability arising from a Relevant GDPR Claim.

16.2.2 The liability of any Indemnifying Party under clause 16.2.1 will not, subject to any adjustment at clause 16.2.3, exceed the proportion that the Indemnifying Party bears to the total number of parties.

16.2.3 The proportions of the Loss allocated between the parties will be adjusted on a fair and equitable basis to take account of any fault of any party/ies.

16.2.4 For the avoidance of doubt:

- (a) clause 16.1 will not apply to any Relevant GDPR Claim;
- (b) clause 17.2 will not apply to exclude or limit a party's liability under this clause 16.2;
- (c) and without affecting clause 13, nothing in this clause 16.2 will affect the liability of any party directly to a Data Subject or other direct claimant under a Relevant GDPR Claim; and
- (d) and without affecting clause 13, no party is required to indemnify any other party in respect of any fines, penalties or other sanctions imposed, or claims

or proceedings brought, by the Information Commissioner against that other party, whether relating to this Agreement or otherwise.

16.2.5 In this clause 16.2:

- (a) **Indemnified Party** means a party who receives a Relevant GDPR Claim;
- (b) **Indemnifying Party** mean the party/ies other than the Indemnified Party/ies;
- (c) **Loss** means any cost, charge, damages, expense, loss or liability;
- (d) **joint** or **jointly** in relation to the liability of a party means that the discharge of that liability by that party discharges the liability of the other party/ies; and
- (e) **Relevant GDPR Claim** is any claim (whether in contract, negligence, breach of statutory duty, other tort or otherwise) by a person under Article 82 of the UK GDPR or otherwise in respect of individuals' rights under the Data Protection Legislation for which the parties are or may be jointly liable as Joint Controllers.

16.3 Indemnification under this agreement is contingent on:

- 16.3.1 the party(ies) to be indemnified (the **indemnified party(ies)**) promptly notifying the other party(ies) (the **indemnifying party(ies)**) of a claim;
- 16.3.2 the indemnifying party(ies) having sole control of the defence and settlement of any such claim; and
- 16.3.3 the indemnified party(ies) providing reasonable co-operation and assistance to the indemnifying party(ies) in defence of that claim.

## 17 Limitation of liability

17.1 Neither party excludes or limits liability to the other party for:

- 17.1.1 fraud or fraudulent misrepresentation;
- 17.1.2 death or personal injury caused by negligence;
- 17.1.3 a breach of any obligations implied by section 12 of the Sale of Goods Act 1979 or section 2 of the Supply of Goods and Services Act 1982; or
- 17.1.4 any matter for which it would be unlawful for the parties to exclude liability.

17.2 Subject to clause 17.1, neither party shall in any circumstances be liable whether in contract, tort (including for negligence and breach of statutory duty however arising), misrepresentation (whether innocent or negligent), restitution or otherwise, for:

- 17.2.1 any loss (whether direct or indirect) of profits, business, business opportunities, revenue, turnover, reputation or goodwill;

17.2.2 loss (whether direct or indirect) of anticipated savings or wasted expenditure (including management time); or

17.2.3 any loss or liability (whether direct or indirect) under or in relation to any other contract.

17.3 Clause 17.2 shall not prevent claims for:

17.3.1 direct financial loss that are not excluded under any of the categories set out in clause 17.2.1; or

17.3.2 tangible property or physical damage.

17.4 Subject to clauses 17.1 and 17.2, the Data Discloser's aggregate liability to the Data Receiver for all claims, losses or damages, whether arising from tort (including negligence), breach of statutory duty, or otherwise, arising under or in connection with this agreement (other than a failure to pay any of the Charges that are properly due and payable and for which the Authority shall remain fully liable), shall be limited in to £1,000,000.00 [The limit on the Data Discloser's liability includes its liability under the indemnity at clause 16.1.]

## **18 Third party rights**

18.1 A person who is not a party to this agreement shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this agreement.

18.2 The rights of the parties to terminate, rescind or agree any variation, waiver or settlement under this agreement are not subject to the consent of any other person.

## **19 Variation**

No variation of this agreement shall be effective unless it is in writing and signed by the parties (or their authorised representatives).

## **20 Waiver**

No failure or delay by a party to exercise any right or remedy provided under this agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of that right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

## **21 Severance**

21.1 If any provision or part-provision of this agreement is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this agreement.

- 21.2 If any provision or part-provision of this agreement is deemed deleted under clause 21.1, the parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

## **22 Changes to the applicable law**

If during the Term the Data Protection Legislation changes in a way that the agreement is no longer adequate for the purpose of governing lawful data sharing exercises, the parties agree that the SPoCs will negotiate in good faith to review the agreement in the light of the new legislation.

## **23 No partnership or agency**

- 23.1 Nothing in this agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, constitute any party the agent of another party, or authorise any party to make or enter into any commitments for or on behalf of any other party.
- 23.2 Each party confirms it is acting on its own behalf and not for the benefit of any other person.

## **24 Entire agreement**

- 24.1 This agreement constitutes the entire agreement between the parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.
- 24.2 Each party acknowledges that in entering into this agreement it does not rely on, and shall have no remedies in respect of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this agreement.
- 24.3 Each party agrees that it shall have no claim for innocent or negligent misrepresentation or negligent misrepresentation based on any statement in this agreement.

## **25 Further assurance**

Each party shall, and shall use all reasonable endeavours to procure that any necessary third party shall, promptly execute and deliver such documents and perform such acts as may reasonably be required for the purpose of giving full effect to this agreement.

## **26 Force majeure**

Neither Party shall be liable to the other for any failure to perform all or any of its obligations under this Contract nor liable to the other Party for any loss or damage arising out of the failure to perform its obligations to the extent only that such performance is rendered impossible by a Force Majeure Event. Where a Party is (or claims to be) affected by a Force Majeure Event it shall use reasonable endeavours to mitigate the consequences of such a Force Majeure Event upon the performance of its obligations under this Agreement, and to resume the performance of its obligations affected by the Force Majeure Event as soon as practicable. If either Party is prevented or delayed in the performance

of its obligations under this Contract by a Force Majeure Event, that Party shall as soon as reasonably practicable serve notice in writing on the other Party specifying the nature and extent of the circumstances giving rise to its failure to perform or any anticipated delay in performance of its obligations.

## **27 Notice**

27.1 Any notice or other communication given to a party under or in connection with this agreement shall be in writing, addressed to the SPoCs and shall be:

27.1.1 delivered by hand or by pre-paid first-class post or other next working day delivery service at its principal place of business; or

27.1.2 sent by email to the SPoC.

27.2 Any notice or communication shall be deemed to have been received:

27.2.1 if delivered by hand, on signature of a delivery receipt or at the time the notice is left at the proper address;

27.2.2 if sent by pre-paid first-class post or other next working day delivery service, at 9.00 am on the second Business Day after posting; and

27.2.3 if sent by email, at the time of transmission, or if this time falls outside business hours in the place of receipt, when business hours resume. In this clause 27.2.3, business hours means 9.00 am to 5.00 pm Monday to Friday on a day that is not a public holiday in the place of receipt.

27.3 This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

## **28 Governing law**

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

## **29 Jurisdiction**

Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims), arising out of or in connection with this agreement or its subject matter or formation.

This agreement has been entered into on the date stated at the beginning of it.

**SCHEDULE 1**

**NOT USED**

## SCHEDULE 2

### Further Detail on Shared Personal Data and Access and Processing Restrictions

#### 2.1 – Personal data in scope

The overall scope is limited to individuals appearing on the HCPC Register whose place of residence, practice location or training institution falls within England. Individuals whose registration lapsed before 2014 will be excluded.

Data item	Public Domain?	Why necessary?
Contact ID	N	<p>Necessary for:</p> <ul style="list-style-type: none"> <li>• Accurate tracking of individuals.</li> <li>• Understand how many AHP's have more than one registration and/or qualification.</li> </ul> <p>Understand how many AHP's transition from one role to another.</p>
HCPC registration number (PIN)	Y	<p>Necessary for:</p> <ul style="list-style-type: none"> <li>• Accurate tracking of individuals, i.e. confirming registrant numbers in ESR</li> </ul> <p>Allow use of additional information from register not available in ESR (e.g. date of registration, education)</p>
Surname	Y	<p>Necessary for:</p> <ul style="list-style-type: none"> <li>• Understanding AHPs are returning to practice compared to the agreed target</li> <li>• Understanding proportion of AHPs who sign up to the return to practice programme re-register with HCPC and re-enter the workforce</li> <li>• Understanding how many returners are involved with the Return to Practice scheme</li> <li>• Analysis of observable patterns either by profession, personal characteristics or geography for AHPs returning to practice</li> </ul>
Forename(s)/given name(s)	Y	
Registration status	Y	<p>Necessary for:</p> <ul style="list-style-type: none"> <li>• Establishing current registrants, including in the NHS</li> </ul>



		Understanding wider labour market, i.e. when registrants leave the register
Date First registered with HCPC	Y	<p>Necessary for:</p> <ul style="list-style-type: none"> <li>Understanding when registrants first enter the register and therefore understanding movements around the wider labour market</li> </ul> <p>Understanding progression into (NHS) workforce</p>
Registration profession	Y	<p>Necessary for:</p> <ul style="list-style-type: none"> <li>Understanding registrant backgrounds and patterns as they relate to profession</li> </ul> <p>Data triangulation – confirms NHS staff registered in given profession</p>
Modality	Y	<p>Necessary for:</p> <p>Analysis of individual professions, specifically on art therapists, music therapists, drama therapists, diagnostic radiographers, therapeutic radiographers (and if available individual sciences and psychological professions)</p>
Organisation where the individual completed studies	N	<p>Necessary to analyse and understand:</p> <ul style="list-style-type: none"> <li>Percentage of new graduates going into the workforce, both in England and in the UK.</li> <li>Length of time between starting and completing education and subsequently transitioning into NHS workforce.</li> <li>How many AHPs are recruited internationally.</li> <li>How many AHPs transition from one role to another</li> <li>Where new graduates move to after qualification, both in terms of sector and location.</li> <li>If AHPs work in the same locations that they qualify in the UK</li> </ul> <p>Above would allow HEE to appropriately plan workforce and ensure that the NHS has the right amount of jobs at the right time (entry level) and in the right place.</p>
Year of birth	N	<p>Necessary to analyse and understand:</p> <ul style="list-style-type: none"> <li>Profile of the NHS workforce relative to the register and in turn the population in terms of age</li> <li>Profile of the trainee workforce in terms of age</li> <li>Observe patterns for transition from training into the NHS workforce in respect of age</li> <li>Understand the retirement pattern for AHPs</li> </ul>

		<p>relative to the workforce composition</p> <p>These would allow HEE to ensure robust workforce planning for the future, understand at what age people leave the workforce, safeguard investment in people through ongoing training to provide high quality care for patients,</p>
Gender	N	<p>Necessary to:</p> <ul style="list-style-type: none"> <li>• Track and respond to the effectiveness of diverse recruitment &amp; retention policies</li> <li>• Understand the profile of the NHS workforce relative to the register and in turn the population in terms of gender.</li> <li>• Understand the profile of the trainee workforce.</li> <li>• Observable patterns for transition from training into the NHS workforce in respect of gender.</li> <li>• Understand the factors (or 'behaviours') that drive movement (particularly joining/leaving the register and joining/leaving the NHS).</li> </ul> <p>These would ensure that HEE is able to play a crucial part within the healthcare system creating a diverse and inclusive workforce and an addition opportunity for all colleagues to be treated fairly and enabled to reach their full potential.</p>
Practice outcode (first half of postcode)	N	<p>Necessary to ensure workforce mapping is accurate with the ability to analyse and understand:</p> <ul style="list-style-type: none"> <li>• Percentage of new graduates that go into the workforce, both in England and in the UK.</li> <li>• Length of time between starting and completing education and subsequently transitioning into NHS workforce</li> <li>• Understand where new graduates move to after qualification, both in terms of sector and location</li> <li>• Understand if AHPs work in the same locations that they qualify in the UK</li> <li>• Understand where AHPs undertake placement</li> <li>• Understand where AHPs live compared to vacancies in the associated area</li> <li>• Understand how long AHPs stay at a single location, where they move after and do they then come back</li> </ul>

		<ul style="list-style-type: none"> <li>Understand proportion of AHPs that train in England but subsequently work in other countries in the UK or abroad.</li> </ul> <p>These would ensure effective workforce planning and that the NHS has the right amount of jobs at the right time and in the right place with appropriate understanding of relationship between training and employment by geography</p>
Recorded qualification	N	<p>Necessary to:</p> <ul style="list-style-type: none"> <li>Track and analyse if AHPs have more than one registration and/or qualification</li> <li>Enables identification of specialists, particularly areas such as prescribing, which is not currently possible in ESR.</li> </ul>
Date when registration lapsed if no longer active.	N	<p>Necessary to analyse and understand:</p> <ul style="list-style-type: none"> <li>Workforce turnover and opportunities for return to NHS practice</li> <li>How many AHPs are dropping off the register</li> <li>What factors (or 'behaviours') drive movement (particularly joining/leaving the register and joining/leaving the NHS).</li> <li>How does the pattern for those joining/leaving the NHS compare to those joining/leaving the register?</li> <li>Retirement pattern for AHPs relative to the workforce composition.</li> </ul> <p>This will allow HEE to ensure robust workforce planning for the future and enables tagging of historical information so when creating flow analytics records do not include those no longer registered at given time</p>

## 2.2 - More sensitive personal data in scope

Data item	Public Domain?	Why necessary?
Nationality	N	To understand reliance and effectiveness on international recruitment

**SCHEDULE 3****NOT USED**

**SCHEDULE 4**

**NOT USED**

**SCHEDULE 5**

**NOT USED**

## SCHEDULE 6

### Appropriate Technical and Organisational Security Measures

*The database will be backed up by HEE daily and stored for the previous 35 days. It will also be backed up weekly and these backups are stored for 90 days. All data is hosted on Azure and is therefore “encrypted at rest”.*

*The Microsoft definition for “Encryption at rest” is as follows:*

*“Encryption is the secure encoding of data used to protect confidentiality of data. The Encryption at Rest designs in Azure use symmetric encryption to encrypt and decrypt large amounts of data quickly according to a simple conceptual model:*

- A symmetric encryption key is used to encrypt data as it is written to storage.*
- The same encryption key is used to decrypt that data as it is readied for use in memory.*
- Data may be partitioned, and different keys may be used for each partition.*
- Keys must be stored in a secure location with identity-based access control and audit policies. Data encryption keys which are stored outside of secure locations are encrypted with a key encryption key kept in a secure location.*

*In practice, key management and control scenarios, as well as scale and availability assurances, require additional constructs. Microsoft Azure Encryption at Rest concepts and components are described below.”*

- The HEE backup policy document states that database backups are encrypted using the Microsoft managed encryption key.*

*Any data is stored anywhere temporarily whilst being moved from the data discloser to the data receiver will be promptly and safely destroyed as soon as possible after the data receiver has received and safely stored the data.*

**SCHEDULE 7**

**NOT USED**



**SCHEDULE 8**

**NOT USED**

## SCHEDULE 9


### Lawful Bases (and Conditions or Exceptions for processing of any Special Categories of Personal Data and Criminal Offence Data) and Legal Power for Data Sharing

	<b>Data Discloser</b>	<b>Data Receiver</b>
Lawful basis: Article 6	<p>Article 6(1)(e) – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.</p> <p>HCPC is exercising official authority in the performance of its functions under Articles 3 and 5 of the Health Professions Order 2001, as more particularly described in clause 2.2.2 and 2.2.3 of this agreement.</p>	<p>Article 6(1)(e) – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.</p> <p>HEE is exercising official authority in the performance of its functions under sections 97 to 99 of the Care Act 2014, as more particularly described in clause 2.2.1 of this agreement.</p>
Condition or Exception: Article 9 (if relevant)		Not relevant.
	Not relevant.	

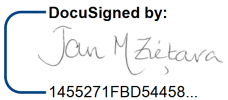
**SCHEDULE 10**

**NOT USED**

Signed by John Barwick for and on behalf of  
HCPC

)   
) Chief Executive and Registrar .....

Signed by Jan Zietara for and on behalf of  
HEE]

)   
) HEE National Programme AHP Lead