

## Data Sharing Agreement

**The Office of the Ombudsman  
and  
Health Information and Quality Authority (HIQA)**

---

### **DATA SHARING AGREEMENT**

---

THIS AGREEMENT is made on **Tuesday, 9 July 2019**

#### **1. BETWEEN**

1. The Office of the Ombudsman, established under the Ombudsman Act 1980 as amended, having its office at 18 Lower Leeson Street, Dublin 2, Ireland
2. The Health Information and Quality Authority (HIQA), a corporate body established under the Health Act 2007 as amended, having its head office at Unit 1301, City Gate, Mahon, Cork, Ireland

#### **2. DEFINITIONS**

The following definitions apply in this Agreement:

"Agreement"	shall mean this data sharing agreement, including these definitions and its recitals and schedules, which is a free standing document that does not incorporate commercial business terms established by the Parties under separate commercial agreements.
"Commencement Date"	has the meaning given to it at the beginning of the Agreement
"Data"	shall mean personal data as defined in the GDPR and the DPA
"Data Controller"	shall have the meaning as defined in the GDPR and the DPA
"Data Processor"	shall have the meaning as defined in the GDPR and the DPA

"DPA" or	
"Data Protection Act"	means the Data Protection Acts 1988 to 2018
"Data Protection Authority"	the relevant data protection authority in the territories where the Parties to this Agreement are established (in Ireland this is the Data Protection Commission)
"Data Security Breach"	shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to shared personal data
"Data Subject"	shall have the meaning as set out in the GDPR and the DPA
"Delete"	shall mean to remove or obliterate personal data such that it cannot be recovered or reconstructed. "GDPR" General Data Protection Regulation (EU) 2016/679.
"Joint Controllers"	shall have the meaning given to such term at Article 26 of the GDPR.
"Parties"	shall mean the Office of the Ombudsman and HIQA
"Processing"	shall have the meaning given to such term in the GDPR and the DSA
"Privacy and Data Protection Requirements"	means the Data Protection Acts 1988 to 2018, the EU Data Protection Directive 95/46/EC, the ePrivacy Regulations 2011 (SI336/2011), the ePrivacy Directive 2002/58/EC, the General Data Protection Regulation (EU) 2016/679 and all applicable laws and regulations relating to the processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Data Protection Commissioner
"Shared Personal Data"	the personal data to be shared between the Parties under clause 4 of this Agreement.
"Subject Access Request"	has the same meaning as "right of access to personal data" in Article 15 of the GDPR
"Technical and Organisational Measures"	means those measures aimed at protecting personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access and against all other unlawful forms of processing (including, as appropriate, the measures referred to in Article 32(1) of the GDPR).

### **3. PURPOSE**

This agreement sets out the framework for the sharing of data between the Parties as Data Controllers under the DPA, the GDPR and any guidance issued by the Data Protection Commission. It defines the principles and procedures that the Parties shall adhere to and the responsibilities the Parties owe each other.

### **4. SCOPE**

- 4.1 In consideration of sharing data with each other, the Parties agree that they will comply fully with their obligations as Data Controllers under the DPA, the GDPR and any guidance issued by the Data Protection Commission.
- 4.2 The Parties agree to co-operate in respect of the sharing of data in compliance with their proposed respective statutory functions under the Health Act 2007 as amended and the Ombudsman Act 1980 as amended.
- 4.3 The Parties consider this data sharing agreement necessary to facilitate the sharing of data and other information pursuant to the MOU dated 9 July 2019 entered into between the Parties. The MOU is designed to promote cooperation between the Parties in areas of strategic and high level operational interest that is to the benefit of service users and to ensure that relevant information which becomes available to one party and which may assist the other party in the performance of its functions is shared between the Parties. One of the specific purposes of the MOU is to allow for the sharing of data in respect of relevant complaints, in areas which may be within the others remit, to the other party. This data will be shared on a consensual basis (as provided for by Article 6(a) of the GDPR).
- 4.4 The Parties agree that this data sharing agreement will serve to benefit the public interest by facilitating the sharing of data as set out in Section 4.3. and other information about elements of health and social care services which fall within the remits of HIQA and the Office of the Ombudsman.
- 4.5 The Parties agree to only share data for the purpose set out in Section 4.3.
- 4.6 The Shared Personal Data must not be irrelevant or excessive with regard to the purpose set out at 4.3.
- 4.7 The Parties shall ensure compliance with applicable national data protection laws at all times during the terms of the agreement.
- 4.8 The Parties shall ensure that this agreement remains fit for purpose, accurate and up to date and it will be reviewed as is required by the Parties. Such a review may be necessary to comply with the Parties obligations under data protection legislation. Any amendments to the agreement shall be signed by the Parties.
- 4.9 The Parties agree to comply with their responsibilities outlined in Schedule 1 of this Agreement with regard to the sharing of data. The Parties agree that Schedule 1 of

this Agreement shall form part of this Agreement and shall have the effect as if it was set out in full in the body of this Agreement.

4.10 The Parties agree that all the required data transfers between the Parties will comply with the Parties' policies and procedures for data transfer. Both Parties will install technical and organisational measures and shall be responsible for the secure and appropriate storage of all data records in their own computing infrastructures. In this regard, both Parties to the Agreement agree to comply with relevant requirements in relation to the processing, keeping, use and disclosure of data under the DPA and in particular to keep such information confidential and to take appropriate security measures against unauthorised access to, or unauthorised alteration, disclosure or destruction of data.

4.11 The Parties 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 agreement. The points of contact for each of the Parties are:

**The Office of the Ombudsman**

The person holding the position of **Data Protection Officer**

The Office of the Ombudsman

18 Lower Leeson Street

Dublin 2

(01) 6395600

**HIQA**

The person holding the position of **Data Protection Officer**

Health Information and Quality Authority

Unit 1301, City Gate, Mahon, Cork

(021) 240 9300

**5. FAIR AND LAWFUL PROCESSING**

5.1 The Parties shall ensure that they process the data fairly and lawfully in accordance with and during the term of the agreement.

5.2 The Parties will only request data that is adequate and not excessive to the purpose of the agreement as set out in Section 4.3.

5.3 Data will be retained by the Parties for no longer than is necessary for the purpose of this agreement as referred to in Section 4.3.

- 5.4 The Parties agree that they must confirm that any third party data processor is GDPR compliant.
- 5.5 The Parties agree to implement appropriate technical and organisational measures to protect against unauthorised access, accidental loss, destruction, damage, alteration or disclosure of data.

**6. DATA QUALITY**

- 6.1 Each party shall be responsible for the quality and accuracy of the data they share with the other party.
- 6.2 The Parties agree that any data discovered to be inaccurate or inadequate for the specified purpose as defined in Section 4.3 will be brought to the notice of the party that supplied the data. The party that supplied the data shall be responsible for correcting the data and notifying the other Party of the correction.

**7. DESCRIPTION OF DATA TO BE TRANSFERRED**

- 7.1 HIQA agrees to supply the Office of the Ombudsman with the following data, which is provided on the basis of consent, in respect of relevant complaints:

Name of person making the complaint
Contact details of person making complaint (address/email address/ telephone number)
Confirmation that consent has been given to transfer contact details
Confirmation they are the service user or otherwise
If not a service user, the relationship with the service user
Name of designated centre/institution

- 7.2 The Parties also agree to share data where it is necessary for the performance of a task carried out in the public interest.
- 7.3 The Parties agree to share other information they deem relevant and necessary for the discharge of their statutory functions, in addition to the data specified in Section 7.1 of this agreement.

**8. PROCEDURES FOR TRANSFER OF DATA**

- 8.1 The Parties agree the following procedures for the transfer of data:  
  
 HIQA will create a data file containing the information as set out in section 7.1. The data contained within the file will be encrypted.  
  
 The data file will be transferred to the Office of the Ombudsman.

The data transfer will be implemented by means of an encrypted file transfer protocol over a secure and robust connection.

Acknowledgement of receipt of the data file will be provided by the Office of the Ombudsman.

- 8.2 The Parties agree that all data transfers between the Parties will comply with the Parties' policies and procedures for data transfer, and will ensure secure transfer of data between organisations. Both Parties will install technical and organisational measures and shall be responsible for the secure and appropriate storage of all data records in their own computing infrastructures.
- 8.3 All data transferred under this agreement will be used solely for the purpose and to the extent specified in this agreement.

## **9. RESTRICTION ON USE OF DATA**

- 9.1 All data and other information shared by the Parties to this Agreement must only be used for the reason(s) specified in the Agreement at the time of disclosure(s) and as set out in Section 4 of this Agreement. The data must not be used for any other purpose without the permission of the party who supplied the data, unless an exemption applies within the DPA, GDPR or the data is required to be provided under the terms of the Freedom of Information Acts 1997, 2003 & 2014 or under the instructions of a court of law.

## **10. LEGAL BASIS FOR DATA SHARING**

- 10.1 All data shared under this Agreement is done so on the basis of data subject consent or where the sharing of data it is necessary for the performance of a task carried out in the public interest as permitted by GDPR Article 6(a) and 6(e).
- 10.2 The purpose of this processing is to enable the Parties to perform their functions under the following legislation:
- The Health Act 2007 as amended
  - The Ombudsman Act 1980.

## **11. DATA SECURITY BREACHES**

- 11.1 The Parties shall have in place their own guidance and policy that must be followed in the event of a data security breach.
- 11.2 The Parties shall appoint a single point of contact (SPoC) for data security breach who shall:
- a) maintain records in relation to data protection requests, decisions made and information exchanged
  - b) maintain records of any data breach
  - c) notify each other of the breach within 24 hours of its discovery

- d) inform the Data Protection Commission within the relevant statutory timeframe when a breach has occurred

The single points of contact for each of the Parties are:

**The Office of the Ombudsman SPoC**

The person holding the position of **Data Protection Officer**

The Office of the Ombudsman

18 Lower Leeson Street

Dublin 2

(01) 6395600

**HIQA SPoC**

The person holding the position of **Data Protection Officer**

Health Information and Quality Authority

Unit 1301, City Gate, Mahon, Cork

(021) 240 9300

- 11.3 The Parties agree to notify any potential or actual loss of data to each SPoC as soon as possible to enable the parties to consider what action is required to resolve the issue in accordance with the data protection laws and guidance.
- 11.4 The Parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any data security breach in an expeditious and compliant manner.

**12. DATA SUBJECTS' RIGHTS**

12.1 Data subjects who are European citizens (European Data Subjects) have the following rights under data protection legislation:

- 12.1.2 right of access (Article 15 GDPR);
- 12.1.3 right to rectification (Article 16 GDPR);
- 12.1.4 right to erasure (Article 17 and 19 GDPR);
- 12.1.5 right to restriction of processing (Article 18 GDPR);
- 12.1.6 right to data portability (Article 20 GDPR); and

- 12.1.7 the right to complain to the relevant data protection authority if the EU Data Subject believes that the Data Controller has not handled the EU Data Subject's personal data in accordance with data protection requirements.
- 12.2 The Parties agree to provide reasonable assistance as is necessary to each other to enable them to comply with a request for any of the actions listed in clause 12.1 and respond to any other queries or complaints from data subjects.
- 12.3 If one party to this Agreement receives a data subject access request, and the personal data is subsequently identified as having originated from the other party, it will be the responsibility of the receiving party to contact the party that supplied the data to determine whether the supplier wishes to claim an exception under the provisions of either the Data Protection Acts 1988 & 2003 or Freedom of Information Acts 1997, 2003 and 2014.
- 12.4 SPoCs are responsible for maintaining a record of individual requests for information, 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 points of contact for each Party are detailed in clause 4.11.

### **13. INDEMNITY**

- 13.1 The Parties to this Agreement agree to indemnify each other against any action arising out of their failure to act within the terms of this Agreement, or in relation to wrongful or negligent disclosure of data generally relating to actions taken in the context of this Agreement.

### **14. RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR THE DATA PROTECTION AUTHORITY**

- 14.1 In the event of a dispute or claim brought by a data subject or a data protection authority concerning the processing of shared personal data against either or both or all Parties ("a Claim"), the Parties will inform each other about any such disputes or claims.
- 14.2 The Parties agree the following:
- 14.2.1 to assist in the investigation and defence of such Claim; and
- 14.2.2 to take all reasonable steps to mitigate any loss or liability in respect of any such Claim.
- 14.3 Each Party shall abide by a decision of a competent court or of the Data Protection Commission which is final and against which no further appeal is possible.



## **15. GOVERNING LAW**

- 15.1 This Agreement will be governed by and construed in accordance with the laws of Ireland, and the Parties submit to the exclusive jurisdiction of the Irish courts for all purposes Connected with this Agreement, including the enforcement of any award or judgement made under or in connection with it.

## **16. WARRANTIES AND UNDERTAKINGS**

- 16.1 Each Party warrants and undertakes that it will:
- 16.1.1 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 including data protection requirements
  - 16.1.2 notify promptly each other of any Data Subject Request
  - 16.1.3 notify promptly each other of any Data Security Breach
  - 16.1.4 assist the other party in complying with its obligations under data protection requirements in relation to any Data Security Breach.

## **17. SEVERANCE AND UNENFORCEABILITY**

- 17.1 If any provision, or part thereof, of this agreement shall be, or is found by any authority, administrative body or court of competent jurisdiction to be, invalid, unenforceable or illegal, such invalidity, unenforceability or illegality shall not affect the other provisions, or parts thereof of this Agreement, and of which shall remain in full force and effect.
- 17.2 If any invalid, unenforceable or illegal provision, or part thereof, would be valid, enforceable or legal if some part were deleted, the provision, or part thereof, will apply with whatever modification is necessary to give effect to the intention of the Parties as appears from the terms of this agreement.

## **18. TERMINATION**

- 18.1 This agreement shall remain in force from the commencement date unless it is superseded by the provisions of a further written agreement concluded between the Parties or is terminated by either party by notice in writing of one month to the other party.
- 18.2 Where this agreement is terminated by either party, the Parties shall ensure that any shared personal data is returned or destroyed in a secure manner.

## **19. CHANGES TO THE APPLICABLE LAW**

In case the applicable data protection and ancillary laws change 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 light of the new legislation.

## **SCHEDULE 1**

### **RESPONSIBILITIES OF PARTIES WHEN SHARING DATA**

In consideration of the parties sharing data with each other, the Parties agree to:

1. The Parties shall request data that is adequate and not excessive to the purpose of this agreement as set out in Section 4.3.
  2. The Parties shall ensure that they process the data fairly and lawfully in accordance with and during the term of the agreement.
  3. The data will be retained by the parties for no longer than is necessary to in accordance with the discharge of their respective statutory functions.
  4. The Parties agree to keep the data secure and confidential.
  5. To ensure data is adequately safeguarded, the parties agree that any third party processing will be covered by contract appointing the third party as Data Processor and the contract will stipulate the following:
    - The conditions under which the data may be processed including but not limited to compliance of the Data Processor with the DPA, the GDPR and any guidance issued by the Data Protection Commissioner
    - The minimum security measures that the data processor must have in place
    - A provision to enable the Data Controller to ensure that the Data Processor is compliant with the terms of the contract in relation to access and security of data.
  6. The Parties will ensure the security of all data stored on all fixed and mobile devices, including desktop computers, servers and mobile computer devices (i.e. laptops, notes, tablets, personal data assistants, Blackberry enabled devices, iPads, iPhones and other smart type devices etc.) and removal storage devices (i.e. CD, DVD, portable hard drives, USB memory keys, Diskettes, ZIP disks, Magnetic tapes etc.).
- 
7. The Parties will ensure that non-electronic data is managed and stored securely.
  8. The Parties agree to implement appropriate technical and organisational measures to protect against unauthorised access, accidental loss, destruction, damage, alteration or disclosure of personal data.
  9. The Parties will ensure that all relevant staff are appropriately trained to handle and process shared personal data in accordance with the technical and organisational measures in their own computing infrastructures. The Parties shall

ensure that all relevant staff are aware and act in compliance with the Agreement and this will be supported by the implementation of appropriate policies and procedures.

10. The Parties agree not to transfer data outside the European Economic Area (EEA) except with the prior written consent of the party who supplied the personal data
11. The Parties will ensure that all data (irrespective of the format that the data is held, i.e. paper, electronic or otherwise) that is no longer necessary, is deleted and disposed of in a secure manner.
12. The Parties agree to comply with the provisions of Section 11 of this Agreement in the event of any accidental or unauthorised data security breach.
13. The Parties agree to comply with the provisions of Section 12 of this Agreement in the event of a data subject request.
14. Where this agreement is terminated by either party, the Parties shall ensure that that any shared personal data is returned or destroyed in a secure manner.

SIGNED on behalf of the

**Health Information and Quality  
Authority**




Phelim Quinn

Chief Executive Officer

Date: 09.07.2019

SIGNED on behalf of

**The Office of the Ombudsman**



Peter Tyndall

Ombudsman

Date: 09.07.2019

