|  |
| --- |
| Data Sharing Agreement |
|  |



**Information Sharing Agreement between**

**Healthwatch England and Local Healthwatch**

**1. Parties to the Agreement**

1. Healthwatch England who are a statutory committee of the Care Quality Commission (“CQC”) established under the Health and Social Care Act 2012, 2nd Floor, 2 Redman Place, Stratford, London E20 1JQ (“HWE”).
2. Local Healthwatch as detailed on page 5. Local Healthwatch is here defined as either the organisation delivering the Healthwatch function in an area, or the Local Authority that commissioned that organisation. It is a decision for each Healthwatch area to assess which party is the controller for personal data and that party must sign this agreement.
   1. This Agreement governs the provision of sharing Personal Data between the Parties to this agreement and explains the purposes and legal basis of the sharing arrangements.
   2. For the avoidance of doubt, The Parties of the Agreement may also be referred to as ‘Each Party’ and ‘the Parties’.

**2. Definitions**

Business day means Monday to Friday from 9.00am to 5:00pm GMT/BST and excludes weekends and UK public holidays;

Contract Personal Data Personal Data processed within the terms of this agreement

Controller means the natural or legal person, public authority, agency or other body, which alone or jointly with others, determines the purposes and means of the processing of Personal Data as defined under Article 4(7) of the UK General Data Protection Regulation

Data Subject means the living person to whom personal data relates, as defined by Article 4(1) of the UK General Data Protection Regulation

Effective Date means the date of signature by both Parties to this Agreement

Personal Data means information relating to an identified, or identifiable, living person as defined by Article 4(1) of the UK General Data Protection Regulation

Privacy Notice relating to Information to be provided to data subjects where personal data are collected from or about the data subjects, as defined within Articles 13 and 14 of the UK General Data Protection Regulation

Relevant Data Protection means any, law, statutes, decree, directive, legislative legislation enactment, order, ordinance, regulation, rule or other binding restriction which relates to the protection of individual with regards to the processing Personal Data to which the Controller or Processor is subject, including the Data Protection Act 2018, the EU General Data Protection Regulation 2018 (GDPR) as amended and incorporated into UK law under the UK European Union (Withdrawal Act) 2018, and the Privacy and Electronic Communication Regulation 2003 (PECR)

UK General Data

Protection Legislation means the EU General Data Protection Regulation 2018 (EU GDPR) as amended and incorporated into UK law and known as the UK GDPR.

Year means a year of operation of this Agreement beginning on the Effective Date or the anniversary thereof and ending 12 months thereafter.

**3. Purpose of the Agreement**

3.1 HWE have a statutory duty under section 45A of the Health and Social Care Act 2008 and for LHW section 221 of the Local Government and Public Involvement in Health Act 2007, which requires personal data to be collected and, where appropriately and lawfully, flow freely between LHW and HWE.

This overarching data sharing agreement specifies the type of and categories of data which may be shared between parties, the terms under which data may flow, the data standards under which all transfers and processing must take place, and clear guidance on minimum expectations, obligations, and status of relationships between parties.

3.2 Each Party recognises it will be necessary to share information, including Personal Data, for the effective and efficient operation of this Agreement.

3.3 The Agreement relates to routine sharing of Personal Data, which will include clarification on how to manage safeguarding requests, and requests from Data Subjects to exercise their individual rights under UK General Data Protection Legislation. Ad-hoc requests from third parties are not covered by this agreement and should be referred to the party that originated the data in question.

3.4 In order to facilitate the free flow of information HWE may provide LHW with centrally managed cloud-based data collection and transfer services. Each Party acknowledges that for the purpose of this Agreement, depending on the specific processing activity taking place it may be defined as either a Controller or Processor, as indicated in the associated Schedule(s).

**4. General principles and data ownership**

4.1 The Parties undertake to comply with Relevant Data Protection legislation, and process Personal Data in compliance with the data protection principles. Both Parties must be able to consistently demonstrate compliance with Relevant Data Protection legislation during the terms of this Agreement.

4.2 Each Party acknowledges and agrees that it is the Controller for any personal data it collects or otherwise acquires in connection with this Agreement and shall be responsible for the storage, processing, transmission and protection of that data, other than when acting as processor on behalf of another party in accordance with specific instructions, such as provision of a survey tool.

4.3 Each Party must provide and maintain relevant Privacy Notices in relation to the Data Subjects, and must ensure that adequate data processing agreements, information sharing agreements, consent mechanisms and information security agreements are in place to manage any necessary relationships.

4.4 Each Party must also ensure that if consent is being relied upon for the basis of processing, that the consent mechanism meets the requirements of Relevant Data Protection legislation, including providing the option to withdraw consent, and is recorded and maintained accordingly.

4.5 Each Party will retain Personal Data for the periods specified in its own retention schedule. Each Party will also consult with the other Party when retention periods are set in relation to any shared information, to avoid discrepancies which could be detrimental.

4.6 Each Party will be responsible for responding to external requests for Personal Data, or any requests from Data Subjects wishing to exercise their individual rights as defined under Relevant Data Protection legislation where they are deemed to be the Controller. However, when any such requests are received, the receiving party will inform the Relevant Data Protection contact of the other party. (This relates only to Personal Data that falls within the remit of this Agreement.)

4.7 This Agreement and the associated Schedule relate to all routine sharing of Personal Data between the Parties. It is agreed the Parties will only collect, process and share the minimum amount of Personal Data necessary to achieve the aim of the sharing need.

4.8 No Personal Data will be shared between the Parties which has not been identified to the Data Subjects by Privacy Notices or similar, unless the sharing is justified by UK General Data Protection Legislation, relevant legislations, or required by law.

4.9 Personal Data that is shared must be adequate, relevant and limited to what is necessary for the purposes of the sharing between the Parties.

**5. Use, disclosure and publication**

5.1 Personal Data will only be processed and shared for the purposes outlined in each Schedule, to achieve the provisions of this Agreement.

5.2 The Personal Data shall not at any time be copied, disclosed, broadcast or disseminated to any other third parties, except in accordance with this Agreement and the associated Schedule.

5.3 No Party to this agreement will share Personal Data obtained from any party to this Agreement with any third party, other than in accordance with a Schedule of this Agreement, without the written authority of other relevant Parties.

5.4 The restrictions on the use or disclosure of Personal Data set out in 5.1-5.3 above will not apply to any data which is required by law to be disclosed, or is disclosed pursuant to an Order of a Court or equivalent authority, or is disclosed in accordance with clause 8 below.

5.5 Access to the Personal Data will be restricted to only those employees or agents of each Party that require it to meet the purpose of the associated Schedule.

5.6 Personal Data shared as part of this Agreement must be stored/recorded by each Party in a structured, commonly used and widely accessible format, unless otherwise agreed.

5.7 Each Party must inform the other of any outcome where the data has been amended, as a result of any Data Subject exercising their rights under Relevant Data Protection legislation.

5.8 Each Party agrees to implement appropriate organisational and technical measures to protect the processing of Personal Data, which must be adhered to at all times, to protect against unauthorised access, unlawful processing, loss, destruction, damage, alteration and disclosure, whether by accidental or deliberate actions. Where possible personal data should be stored in an encrypted, fully anonymised or pseudonymised format.

**6. Method of transfers of Personal Data between the Parties, and data storage**

6.1 Personal Data will be transferred for the purpose of the associated Schedule by appropriate secure methods. Personal Data should, wherever possible, be stored and processed within the UK, or within the European Economic Area (EEA). Wherever possible, it should not be transferred to, or accessed by any organisation or individual outside of the UK or EAA. Particularly, the Parties will ensure that they have done everything reasonable to put in place measures to:

6.1.1 reduce the likelihood of unauthorised interception of the data,

6.1.2 deter deliberate or opportunist attacks,

6.1.3 promote discretion in order to avoid unauthorised access,

6.1.4 maintain the integrity of the data,

6.1.5 and otherwise guard against any compromising of the confidentiality, integrity, and availability of the data.

6.2 The method of transfer for any sharing of Personal Data from LHW to HWE and vice versa, will be set out in the appropriate Schedule, and HWE Data Sharing Guidance should be followed at all times.

**7. Data breach Incident notification**

7.1 Paragraphs 7.2 to 7.5 apply only in relation to personal data being jointly processed by the parties, or where personal data is being processed by one party on behalf of the other.

7.2 Any security incidents or data breaches involving such data must be communicated between the relevant Parties at the earliest opportunity, and in any event within 48 hours.

7.3 The Party making the discovery of any event above will, without delay

7.3.1 Inform the other Party of the details

7.3.2 Take steps to investigate the cause and follow the HWE breach reporting guidelines.

7.3.3 Minimise any harm to data subjects

7.3.4 Identify any opportunities for improvement and train staff in lessons learnt

7.4 The Parties will assess the potential implications of any data security incidents and, if necessary, will:

7.4.1 Inform the Data Subject(s) concerned

7.4.2 Advise the Data Subjects(s) of their rights

7.4.3 Provide the Data Subject(s) with appropriate support

7.5 Where required by Relevant Data Protection legislation a breach will be reported to the Information Commissioner’s Office by the Controller within 72 hours of the Controller discovering or being notified of the breach.

**8. Relationships between HWE and LHW**

8.1 In accordance with the statutory obligations under Relevant Data Protection legislation each Party shall give reasonable assistance as is necessary to the other in order to enable the Party to:

8.1.1 Comply with requests from Data Subject(s) to exercise their rights under Relevant Data Protection legislation including, but not limited to, Data Subject Access requests;

8.1.2 Comply with requests from individuals made under the Freedom of Information Act 2000 or the Environment Information Regulations 2004;

8.1.3 Respond to actions and penalties served upon them by the Information Commissioner;

8.1.4 Respond to complaints from Data Subjects;

8.1.5 Investigate any breach or alleged breach of the Relevant Data Protection legislation.

8.2 Under Relevant Data Protection legislation, Data Subjects have a right of access (as well as other rights) to Personal Data held about them. The receipt by one Party of any Data Subject requests for access to Personal Data covered by this Agreement must be reported at the earliest opportunity to the relevant Information Compliance Officer or other such nominated officer representing the other Party.

8.3 It is the responsibility of the Controller to arrange the relevant response to that request.

8.4 This Agreement also acts in fulfilment of part of the responsibilities of a Controller as defined by Relevant Data Protection legislation.

**9. DISPUTE RESOLUTION AND VARIATION**

9.1 Any disputes arising will be referred first to the operational contacts of the Parties and, if not resolved within 10 working days, will then be escalated to the signatories to this Agreement. The parties note the terms of Clause 10.2 below.

9.2 No variation of this Agreement shall be effective unless it is in writing and signed by authorised signatories of both Parties.

**10. Review and Termination**

10.1 This Agreement shall run conterminously with the trademark agreement and shall be reviewed in tandem with it, at the request of either Party, or when the processing or purposes of the shared Information change.

10.2Either Party shall be entitled to terminate this Agreement by giving not less than 30 calendar days written notice.

10.3 Within 30 calendar days following termination of this Agreement by either Party, HWE shall, and without prejudice to Clause 5.4 destroy all Contract Personal Data in its possession or control unless prohibited from doing so by any applicable law or retain such Data by HWE by agreement by both parties, and confirmed in writing.

10.4 The expiry or termination of this Agreement for whatsoever reason shall not affect such of the provisions of it as are expressed to operate or have effect after its termination and shall be without prejudice to any right of action already accrued to either Party in respect of any breach by the other Party of the terms and conditions set out in this Agreement.

**11. Governing law**

12.1.1 This Agreement shall be governed by and construed in accordance with English law.

[X] Schedule 1: Information sharing between HWE – LHW using Data Sharing Platform

[X] Schedule 2: Information Sharing between HWE and LHW using Healthwatch National Data Store (HNDS)

[X] Schedule 3 – Specific restrictions and safeguards

**Signatories:**

|  |  |  |  |
| --- | --- | --- | --- |
| HEALTHWATCH ENGLAND | | LOCAL HEALTHWATCH | |
| Name: | Chris McCann | **Name:** |  |
| Signature: |  | **Signature:** |  |
| Date: | 06/12/2022 | **Healthwatch name:** |  |
|  |  | **Date:** |  |

|  |
| --- |
|  |

**Schedule 1 Information Sharing Agreement between HWE and LHW using SMART Survey**

|  |  |
| --- | --- |
| **Nature of the processing:** | Collection and sharing of standard and special category data between LHW and HWE using SMART Survey. |
| **Purpose of the processing:** | LHW have a statutory obligation to collect data and share it with HWE. Both LHW and HWE use it to perform research to fulfil their role as public health and care champions for UK citizens. |
| **Purpose(s) of the data transfer and further processing:** | Some data is collected directly from users, but the majority is collected by LHW who must then share this data with HWE. |
| **Standard category of personal data:** | The main categories of personal data shared for the purpose of this Agreement include, but are not limited to, the following:  Name (User, patient, family member, friend, HCP)  Date of birth  Home Address  Email Address  Contact Numbers |
| **Special categories of personal data:** | Health information  Sex life or sexual orientation  Actual or alleged criminal activity/offences  Religion/Beliefs  Ethnicity |
| **Controller/Processor designation:** | Both parties are deemed to be Controllers in their own right for the data they collect, as in accordance with 4.2 of this agreement. |
| **Legal Basis for standard category data:** | (1)(a) – consent    (1)(e) – necessary in the exercise of official authority vested in the controller ie carry out LHW statutory functions under section 221 of the Local Government and Public Involvement in Health Act 2007 |
| **Legal basis for Special Category data:** | (2)(a) – explicit consent    (2)(h) – necessary for the management of health or social care systems on the basis of UK law\* and subject to a duty of confidentiality under the rule of law as established under English common law and enforceable through civil courts |
| **The frequency of the transfer:** | Real-time |
| **The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period** | Healthwatch and Healthwatch England will operate to their data protection and retention policies. |
| **Details of transfers to sub-processors:** | None. |
| **Data protection supervisory authority:** | Information Commissioner’s Office |

**SCHEDULE 2**

Information Sharing Agreement between HWE and LHW using Healthwatch National Data Store (HNDS)

|  |  |
| --- | --- |
| **Nature of the processing:** | 1. Upload of data collected by a Local HW using Healthwatch England’s data sharing platform into HNDS 2. Collection and transfer of data from Healthwatch England website to HNDS 3. Analysis of the data by Healthwatch England and local Healthwatch 4. Local Healthwatch can download datasets from HNDS that were a) collected by their Healthwatch and/or b) data collected by HWE where the data subject has selected their Healthwatch for the purposes of carrying out their statutory functions (eg analysis and info and signposting) 5. Public access to and aggregation of local, regional and national level statistical data in the HNDS ie not containing personal data. |
| **Purpose of the processing:** | 1. Enable local Healthwatch to fulfil their statutory function of sharing the views of local people with Healthwatch England 2. Enable local Healthwatch to access data in order to fulfil their statutory functions of information and signposting, making those views known, and making reports and recommendations 3. Enable Healthwatch England to fulfil their statutory function of using the analysis of the collective data of local HW to inform policy and service change |
| **Accessing data** | **Healthwatch England**  Nominated responsible person(s) in Healthwatch England have super administrative rights in order to administer HNDS. Our supplier, Circle Interactive (Company number 05540067) has access in order to carry out maintenance and security updates.    Healthwatch England’s Research Team has access to the data in order to fulfil our statutory function of analysing the collective data of local Healthwatch.    The system has a log of who accesses the HNDS.    **Local Healthwatch**  Local Healthwatch can upload their local data, map it to the Healthwatch England taxonomy. Healthwatch England will ensure this data is stored securely in accordance with its data protection policies.    Local Healthwatch can only access qualitative data that has been a) collected by the local Healthwatch or b) where the data subject has selected their local Healthwatch when submitting data to HWE |
| **Standard category of personal data:** | The main categories of personal data collected for the purpose of this Agreement include, but are not limited to, the following:  Name (User, patient, family member, friend, HCP)  Date of birth  Home Address  Email Address  Contact Numbers |
| **Special categories of personal data:** | Health and wellbeing information  Sex life or sexual orientation  Actual or alleged criminal activity/offences  Religion/Beliefs  Ethnicity |
| **Controller/Processor designation:** | **Data Controller**  HWE are overall Controllers for personal data held on the HNDS system.    HWE are Controllers in respect of personal data that they create, collect, upload to, or download from HNDS    Each LHW is also Controller, in their own right, for the personal data that they create, collect, upload to, or download from HNDS, as in accordance with 4.2 of this agreement.    **Data Processor**  Our supplier, Circle hosts the HNDS on its server which is situated within the EEA |
| **Legal Basis for standard category data:** | (1)(a) – consent    (1)(e) – necessary in the exercise of official authority vested in the controller ie carry out LHW statutory functions under section 221 of the Local Government and Public Involvement in Health Act 2007 and HWE statutory functions under Section 45A of the Health and Social Care Act 2008 |
| **Legal basis for Special Category data:** | (2)(a) – explicit consent    (2)(h) – necessary for the management of health or social care systems on the basis of UK law and subject to a duty of confidentiality under the rule of law as established under English common law and enforceable through civil courts |
| **The frequency of the transfer:** | Real time in the case of data generated from websites or integrated systems; monthly uploading data by local Healthwatch to HNDS or as agreed between the parties |
| **The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period** | Healthwatch and Healthwatch England will operate to their data protection and retention policies. |
| **Details of transfers to sub-processors:** | None. |
| **Data protection supervisory authority:** | Information Commissioner’s Office |

**SCHEDULE 3 - Specific restrictions and safeguards:**

The following measures are required for any other party to this agreement (i.e. a party that is in receipt of personal data from another party).

**Technical measures**

* Wherever possible pseudonymisation and encryption of personal data
* All devices which access personal data should be protected with appropriate cyber-security measures to prevent against data loss and unauthorised access, including but not limited to firewalls and anti-virus software.
* Measures should be in place for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident (each party to take adequate backups for the personal data within their custody).
* Adequate technical access controls should be in place to prevent against unauthorised access.
* Reasonable and proportionate monitoring of systems and activities to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services.
* Processes should be in place for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
* All records should be transferred securely using methods such as encrypted link forwarded to email (unprotected data is not to be attached to emails).
* Appropriate measures should be in place to protect data during storage.
* Appropriate and proportionate physical security should be in place at locations where personal data are processed.
* Database activity and system logs should be maintained.
* Measures for ensuring system configuration, including default configuration should be in place.
* IT security governance and management should be in place to ensure systems remain protected.

HWE has the following measures in place. Other parties to this agreement should consider adopting these measures where possible:

* Remote devices should only access personal data by way of secure encrypted connection such as a Virtual Private Network.
* All portable devices should be encrypted

**Organisational measures**

* Appropriate policies and procedures, should be in place to cover areas such as data protection, information security, acceptable use, remote working, data security, breach reporting and retention.
* A robust organisational process must be in place to remove access when staff change role or leave employment.
* All staff and agents are to be trained in their obligations with regards to GDPR and how to manage data breaches and when requests are received from data subjects.
* Appropriate governance and oversight of systems and processes should be in place to ensure integrity, availability and confidentiality of personal data is maintained.

Healthwatch England

National Customer Service Centre

Citygate

Gallowgate

Newcastle upon Tyne

NE1 4PA

www.healthwatch.co.uk 

t: 03000 683 000

e: enquiries@healthwatch.co.uk

 @HealthwatchE

 Facebook.com/HealthwatchE