Information Sharing Protocol

Change, Grow, Live / Reach Out Recovery

And

Birmingham Community Pharmacy

Contents **Page**

1 SUMMARY

1.1.1 This Information Sharing Protocol (ISP) sets out the obligations of all staff in the organisations signing up to it, as listed in *section 2* and Annex 1:

- to share or disclose information about Service Users/Clients/Patients, and
- to handle information securely at all times and to maintain confidentiality in relation to the arrangements for this ISP agreement.

2 PARTIES TO THE INFORMATION SHARING PROTOCOL

2.1 The parties to this ISP are those that have signed the Declaration of Acceptance and Participation (DAP) at the end of this document (see Annex 1) and are listed below:

- Reach Out Recovery (as part of CGL, Tower Point, 44 North Road, Brighton, East Sussex BN1 1YR)
- Birmingham Community Pharmacy

2.2 This list and the details of each organisation's Designated Persons(s) as shown in Annex 2 will be updated and reissued on an annual basis (this Protocol will be reviewed by the parties once annually 12 months from the commencement date).

.

3 SCOPE OF THE INFORMATION SHARING PROTOCOL

3.1 This ISP has been developed to establish comprehensive and consistent standards of information sharing within and across the signatory organisations with respect to the appropriate treatment of personal and other confidential information which all signatory organisations will adopt.

3.2 All signatories to this ISP must ensure that rights of all parties are upheld in a fair and proportionate way by clear and consistent practice in accordance with:

- The duties and powers (expressed or implied) arising from relevant legislation incumbent on statutory bodies or their sub-contractors (see also *section 4* below)
- The Human Rights Act 1998
- The Data Protection Act 1998, and
- The Freedom of Information Act 2000.

3.3 **Operational Information Sharing Agreements (OISA):**

This ISP may be supplemented by specific Operational Information Sharing Agreements where there is a requirement for the disclosure and sharing of personal information between two or more signatories of the ISP. The OISA will detail the specific purpose(s) for information sharing and define the processes by which information will be exchanged, monitored and managed at the operational level.

Should this be a requirement in line with main contract provisions, all parties will discuss and agree format and content for the OISA.

3.4 **Other agreements or contracts:**

Wherever it is a requirement to disclose personal information between organisations as part of a formal funding/contractual arrangement, all parties must be made aware of this ISP and where drawn up and part of the ISP, associated OISAs as part of the funding/contractual process and not subsequent to the grant/contract being completed.

4 INDEMNITY

4.1 All parties undertake to indemnify each other against all losses, costs, expenses, damages, liabilities, demands, claims, actions or proceedings arising out of failure to apply any of the statements or procedures set out in this Protocol or associated OISAs or out of the use of information provided as a result of this Protocol and associated OISAs unless the damage can be shown to arise as a result of the original disclosure in which case the originating organisation must bear the consequences or unless the damage can be shown to arise from an organisation not adhering to the procedures contained within this Protocol or OISAs, in which case that organisation must bear the consequences incurred by themselves and any other parties in this Protocol or OISAs.

4.2 By signing this Protocol, all parties agree to accept and implement it and to adopt the statements and procedures contained within it.

4.3 Any breaches of, or other complaints about, this agreement will be dealt with in accordance with the processes described in the ISP.

5 DESIGNATED OFFICERS

5.1 Each signatory organisation must appoint a Designated Officer who may be the organisation's Caldicott Guardian, Data Protection Officer or other relevant manager.

5.2 The Designated Officer is responsible for ensuring that their organisation complies with legal and other appropriate requirements, obligations and guidance in relation to information processing and sharing, including those outlined in this Protocol and other related OISAs.

5.3 The Designated Officer will also be responsible for:

- internal information governance and/or operational procedures and processes (see *section 6*)
- dissemination and implementation and monitoring of this Protocol and any related OISAs
- receiving requests for changes to any aspect of this Protocol, circulating them for a response, obtaining agreements for the changes and reissuing amended documents where necessary, and
- ensuring the list of signatories and other Designated Officers as shown on the DAP are kept up to date and appropriately circulated.

6 INFORMATION GOVERNANCE

6.1 Each signatory organisation will have in place appropriate information governance and/or operational policies and procedures that will facilitate effective and secure processing of personal information.

7 TYPES OF INFORMATION TO BE SHARED

7.1 The signatories wish to share the following types of information relating to Service Users/clients/patients:

- service user files, records, electronic database records and data held by each organisation relating to the information sharing arrangement for this ISP
- treatment records, medical and clinical records associated and linked to or forming part of each service users' record as above
- any other confidential or sensitive data relating to each service users' records or processing information in relation to their ongoing treatment, referral to either organisation in relation to their treatment or associated provider(s) relevant to their treatment journey

8 SERVICE USER PRIVACY AND CONFIDENTIALITY

8.1 The Human Rights Act 1998, the Data Protection Act 1998 and common law duty of confidence impose obligations on users of personal information. Signatories will ensure that the security and confidentiality of these data are safeguarded and there is no unlawful disclosure.

8.2 All Service Users have the right to expect that information disclosed by them or by other parties about them will be treated with confidentiality according to the common law duty of confidence.

8.3 Information given or received in confidence for one purpose may not be used for a different purpose or passed on to anyone else without the consent of the provider of the information.

8.4 However, all signatory organisations must ensure that their staff are aware that the above (*section 8.3*) is not an absolute right and that they are obliged to disclose information when there is a statutory duty or an overriding public interest in sharing.

8.5 Organisations must also ensure that their staff are aware of and adhere to limits imposed on wider disclosure by other signatories when considering sharing information with organisations that have not signed up to this ISP or related OISAs.

9 SERVICE USER CONSENT

9.1 Consent is necessary for the sharing of the following information on Service User's about their treatment in most situations, however for the purposes of this agreement it should be accepted that unless otherwise stated the arrangements contained in this agreement will override the requirement for

each organisation to obtain additional written consent for the sharing of information specifically relating to this agreement.

9.2 When obtaining the Service User's consent, it must be explained in such a way that they understand the need for obtaining and sharing their personal information, the possible consequences of refusing or withdrawing consent and the circumstances when their consent may be overridden or consent not sought to share information.

9.3 If a Service User refuses consent to share their information, and where it is lawful to share such information in spite of refusal, the organisation must record the refusal of consent and the reasons for overriding that refusal in the service user's case record.

9.4 Where possible, consent should be obtained in writing. Ideally, each signatory organisation should have a consent form, a signed copy of which is kept in the Service User's file. When verbal consent has been obtained, this must be clearly recorded in the file and written consent obtained at the earliest opportunity.

9.5 Service User consent is not necessary for sharing depersonalised or anonymous data from which individuals cannot be identified or for sharing aggregated data.

10 SERVICE USER AWARENESS

10.1 Each signatory organisation must have an appropriate Privacy Notice that explains to all Service Users what information is being collected and recorded about them, the reasons for doing so and with whom it may be shared and why.

10.2 Each signatory organisation must ensure Service Users are aware of their rights with respect to the Data Protection Act 1998, the Human Rights Act 1998 and the Freedom of Information Act 2000, and how these rights may be exercised. The Privacy Notice should explain how Service Users can ask to see their information.

11 COMPLIANCE WITH THE DATA PROTECTION ACT 1998

11.1 Each signatory organisation must keep their notification with the Information Commissioner's Office (ICO) up to date.

11.2 The ICO registration number and notification renewal date must be entered on the ISP. It is the responsibility of each organisation to ensure that ISP entries are kept up to date and accurate.

11.3 Each signatory organisation must respect the rights of individuals with respect to their personal data and be aware of the conditions for processing personal and sensitive personal information as defined by the Act.

11.4 Each signatory organisation must adhere to the eight data protection principles with respect to processing personal information.

11.5 All signatory organisations will respond to valid subject access requests within the statutory time limit of 40 calendar days by providing the information requested subject to any exemptions.

11.6 If a subject access request is received for information held by another signatory organisation (but the information is not also held by the organisation receiving the request), the request will be forwarded to enable that organisation to respond within the statutory time limit.

12 INFORMATION SECURITY

12.1 Each signatory organisation must ensure that appropriate technical and organisational measures are in place to protect against unauthorised or unlawful processing of personal information and against accidental loss or destruction of or damage to personal information.

12.2 Each signatory organisation must have in place the appropriate level of security commensurate with the sensitivity and classification of the information to be shared and stored.

12.3 Each signatory organisation must ensure that system-specific policies and mechanisms are in place to address access levels, physical security of information, security awareness and training, security management, systems development and data transfer and transport.

13 BUSINESS PROCESSES AND PROCEDURES

13.1 **Format of information:**
The information will be shared electronically via PharmOutcomes or other such arrangements as agreed by each of the signatory organisations to fit in line with the requirements of this ISP.

13.2 **Frequency of transfer:**
Information will be shared monthly, and/or as otherwise required by the signatory organisations in line with the requirements of this ISP.

13.3 **Methods of recording and holding:**
The received shared information will be stored so the data are protected and cannot be accessed by unauthorised persons. All approved officers within CGL and NCC must ensure that they take appropriate measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data.

13.4 **Use of service user personal information for marketing purposes:**
Signatory organisations may not use service user personal information shared between organisations as a result of this ISP and related OISA for the purposes of marketing and/or commercial activities unless such use is stated in the organisation's notification with the ICO and services users have been made aware of this purpose and their explicit consent obtained.

13.5 **Recording of disclosure decisions:**
Every request for disclosure, whether fulfilled or not, must be fully recorded and clearly referenced to the evidence and information on which the decision to share or not share was based.

14 DATA QUALITY ASSURANCE

14.1 Each signatory organisation is responsible for the quality of the personal data it obtains, records, holds, uses and shares and will have appropriate procedures in place for monitoring and ensuring standards.

14.2 All signatory organisations receiving the shared information are responsible for applying relevant data quality checks before using the information.

14.3 If information is found to be inaccurate, the signatory organisation discovering the inaccuracy must notify the Designated Officer of the organisation sharing the information. The Designated Officer will ensure that the source data are corrected and will notify all recipients, who will be responsible for updating the information.

15 STAFF REQUIREMENTS (this applies to all other types of workers ie volunteers, consultants, contractors etc)

15.1 The conditions, obligations and requirements set out in this ISP will apply to all appropriate staff, agency workers, consultants, volunteers and contractors working within or on behalf of the signatory organisations.

15.2 Staff contracts must contain appropriate confidentiality clauses that detail the possible consequences of unauthorised or inappropriate disclosure of service user information.

15.3 Each signatory organisation must ensure that all appropriate staff has the necessary level of DBS clearance in line with regulated activities and roles being performed.

15.4 Each signatory organisation must ensure that all relevant staff receive training, advice and ongoing support in order to understand the implications of and implement this ISP and where appropriate or necessary any related OISAs, the underpinning legislation for information sharing, common law duties and appropriate codes of practices and other organisational information governance guidance.

16 CONCERNS OR COMPLAINTS

16.1 Any concerns or complaints received from service users relating to the processing of their personal information and any concerns or complaints from practitioners relating to the implementation of this ISP must be dealt with promptly in accordance with the internal complaints procedure of the organisation and, where appropriate, the conditions outlined in *section 20*.

17 NON-COMPLIANCE AND BREACHES OF SECURITY

17.1Non-compliance and breaches of security (internal)

17.1.1 Instances of internal non-compliance and breaches relating to information shared as a result of this ISP must be logged and reported to the relevant

Designated Officer. They should be dealt with promptly in accordance with the organisation's information governance or operational policies and procedures.

17.1.2 Incidents relating to information shared as a result of this ISP that should be logged and reported include, but are not restricted to:

- refusal to disclose information to signatories of this ISP
- conditions being placed on disclosure
- disregard of agreed policies and procedures
- disregard of the views and rights of service users
- inappropriate, unauthorised or unlawful disclosure
- inappropriate or unauthorised access, and
- theft, loss or damage to information or other breaches of security.

18 SHARING OF INFORMATION WITH NON-SIGNATORIES

18.1 The disclosing organisation retains ownership of the information. Any recipient organisation must not disclose it to organisations that have not signed up to this ISP or any related OISA without the express agreement of the disclosing organisation and service user.

19 EFFECTIVE DATES AND REVIEW OF PROTOCOL

19.1 This Protocol is considered to be effective from the date the organisations signed the ISP.

19.2 This protocol will cease to be current, and therefore will be in need of a formal review, no later than 12 months from the implementation date at *section 22.1*.

19.3 Both the implementation date and the end date are on the cover of this document.

Annex 1: Information Sharing Protocol

Effective from …1st March 2018…..….. (date) **to…28th February 2020…….** (date)

DECLARATION OF ACCEPTANCE AND PARTICIPATION

Signed by, for and on behalf of:

Organisation	**CGL / Reach Out Recovery**
Name	**Kirsty Mason**
Position	**Business and Partnership manager**
Contact details	**Reach Out Recovery** **Scala House** **36 Holloway Circus** **Birmingham** **B1 1EQ**
Data Protection act 1998 ICO registration number & date of renewal	**Z9124986** **13th July 2018**
Signature	
Date	

Organisational contract for information sharing	**Kevin Ratcliffe**
Position	**Consultant Pharmacist**
Contact details	**Telephone number: 0121 227 5890**
	Email: kevin.ratcliffe@cgl.org.uk
	Address: Reach Out Recovery **Scala House** **36 Holloway Circus** **Birmingham** **B1 1EQ**

DECLARATION OF ACCEPTANCE AND PARTICIPATION

Signed by, for and on behalf of:

Organisation	
Name	
Position	
Contact details	
Data Protection act 1998 ICO registration number & date of renewal	
Signature	
Date	

Organisational contract for information sharing	
Position	
Contact details	**Telephone number:**
	Email:
	Address: