Information Sharing Agreement

GDPR COMPLIANT

Version 5~~3~~
AUGUST
2018

Contents

Operational Agreement for Information Sharing

1. Scope and Purpose

This is an Operational Agreement (OA) for information sharing between signatories of the High Intensity Network (HIN). As signatories to the HIN, the participating partner organisations have agreed to share information in a way that complies with the following

General Data Protection Regulation (GDPR) 2016

Data Protection Act 2018

Records Management Code of Practice for Health and Social Care 2016

Health and Social Care Act 2012

Human Rights 1998

Caldicott Principles and Recommendations

Freedom of Information Act 2000

Common Law

This OA covers the exchange of information between:

NHS Mental Health Trusts

Police Forces in England and Wales

Ambulance Trusts

NHS Acute Trusts (A&E)

and any other authorised operational partners that delivery mental health services on behalf of the above statutory organisations.

It outlines and supports the information sharing processes between partner organisations involved in the identification of, risk assessment of, management of and response to individuals living in all of our communities whose **behavioural disorders** pose a direct or indirect high risk of:

Death or serious harm to themselves (including death by misadventure)

Death or serious harm to others

Community impact (including unnecessary/inappropriate/avoidable impact upon public services)

Criminal or anti-social behaviour

It details the specific purposes for sharing and the personal information being shared, the required operational procedures and the legal justification that underpins the disclosure/exchange of information.

Partners may only use the information disclosed to them under this OA for the specific purposes/processes set out in this document.

2. Data Protection Impact Assessment

(Formerly known as '*Privacy Impact Assessment'*)

Prior to drawing up this agreement the partner organisations are encouraged to complete (jointly or separately) a Data Protection Impact Assessment (DPIA), formerly known as a Privacy Impact Assessment. We recommend that all partner organisations use our DPIA document as the template for their agreed DPIA.

This document can be found in **Document 2** and in the Set-Up resources accessed via www.highintensitynetwork.org.

3. Privacy Notice

(*Formerly known as 'Fair Processing Information'*)

The partners to this agreement recognise their legal duty to provide information to individuals about what data concerning them is being shared and recorded within the activities of the HIN. We recommend that all partner organisations use our Privacy Notice as the template for their agreed document.

This document can be found in **Document 3**.

4. Objectives

1. The objectives of sharing the information covered by this agreement are

   - To ensure **accurate identification** of people within our communities who are displaying highly impactful behaviour (high frequency, high risk, high harm) caused by enduring mental illnesses and behavioural disorders.
   - To ensure that public agencies work more effectively together to **support and safeguard** these identified individuals and other people affected by their behaviour.
   - To **minimise the inappropriate and unnecessary impact** of these individuals upon public services and the community.
   - To **prevent suicide and reduce accidental suicide/misadventure risks** posed by these individuals when in crisis.
   - To **improve the quality of clinical care and promote recovery**
   - To **monitor the progress** of each individual service user over time.
   - To **create personalised crisis response plans** for each service user that can be used confidently by frontline emergency service personnel.
   - **Avoid use of the criminal justice system to regulate behaviour** wherever possible

5. Individuals impacted by this ISA

The service users and/or carers which this Information Sharing Agreement relates to include:

- Individuals whose behaviour causes high risks of suicide, accidental death, as well as high levels of community impact and demand on public services.

The benefits to the Service Users include:

- More intensive care.
- Decreased risk of self-harm and accidental suicide.
- Decreased risks of encountering the police and criminal justice system.

6. Legal Justification for Sharing

CONFIDENCE TO SHARE:

Staff should not hesitate to share personal information at any time, with any person, if they have an honestly held belief that by doing so it will prevent death, serious harm or abuse to any party.

There are 6 'Lawful Bases' for sharing data within the **General Data Protection Regulation (GDPR) 2018**. Due to the unique characteristics of this small cohort of service users, one or both of two lawful bases apply:
They are:

Article 6(1)(d): Vital Interests

"Processing is necessary in order to protect the vital interests of the data subject or of another natural person"

Explanation:
Due to the behavioural complexities of this cohort of patient, it is impossible to predict when their next emotional crisis will occur, but it is always highly likely that another crisis event will occur as these disorders are long term, life long conditions. Therefore, sharing information about them is essential, both when they are in crisis but equally when they are not (so that all efforts can be made to prevent or minimise the harm of the next crisis event). As crisis events are typically high harm/risk events, it is essential to share information about each individual, to prevent higher than likely risks of suicide or serious injury.

Article 6(1)(e): Public Task/Exercise of Official Authority

"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"

Explanation:
Sharing information to prevent high harm/events is also essential so that public services can minimise the impact that these individuals have on public services, most notably emergency healthcare teams. By protecting these teams, we can ensure that they are providing the best possible public service to members of the public who genuinely need help. Providing the best healthcare service to a community is a core public

task of the NHS (A&E/Ambulance/Mental Health). Preventing crime and disorder, reducing risk and vulnerability and keeping the peace are core tasks of the police service.

The **GDPR 2018** also allows for the processing of "special categories of personal data" in certain circumstances. Of relevance to this cohort of patients is that special categories of personal data include data concerning racial or ethnic origin, religious beliefs and health, Information about offences committed by an individual, and interactions with the criminal justice system (covered by Article 10 GDPR) may also be processed. The circumstances where such processing is allowed, includes where:

Article 9(2)(c): Vital Interests

"Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent."

Explanation:
As above for Article 6(1)(d): Vital Interests.

Article 9(2)(g): Public Interest in Upholding the Law

"Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".

Explanation:
Sharing information about the health of this cohort of patients will fall within legal bases.

Article 9(2)(h): Health or Social Care or Treatment

"Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3".

Explanation:
Sharing information about the mental and behavioural health of this cohort of patients will:
1. Enable more accurate medical diagnoses to a cohort of patient long associated with poor diagnosis.
2. Identify the need for/facilitate the provision of different health or social care support for their complex needs.
3. Enable improved crisis-care planning. This will enhance our preventative approach and suicide reduction
4. Enable us to develop a specialist Mental Health crisis response IT system which will improve the consistency and quality of crisis-care we provide this patient group.

Article 9(2)(i): Public Interest in Public Health

"Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy."

Further detail in relation to the circumstances where special categories of personal data can be shared is set out in Schedule 1 of the **Data Protection Act 2018**. Of relevance to this cohort of patients is:

Part 1 Section 2: Health or Social Care Purposes

"(2) In this paragraph "health or social care purposes" means the purposes of:
(a) preventive or occupational medicine,
(b) the assessment of the working capacity of an employee, (c) medical diagnosis,
(d) the provision of health care or treatment,
(e) the provision of social care, or
(f) the management of health care systems or services or social care systems or services."

Part 2 Section 7: Administration of Justice

"This condition is met if the processing is necessary:
(a) for the administration of justice, or…"

Part 2 Section 10: Preventing or Detecting Unlawful Acts

"(1) This condition is met if the processing—
(a) is necessary for the purposes of the prevention or detection of an unlawful act,
(b) must be carried out without the consent of the data subject so as not to prejudice those purposes, and
(c) is necessary for reasons of substantial public interest."

Part 2 Section 18: Safeguarding of Children and Individuals at Risk

"(1) This condition is met if—
(a) the processing is necessary for the purposes of—
(i) protecting an individual from neglect or physical, mental or emotional harm, or
(ii) protecting the physical, mental or emotional well-being of an individual,
(b) the individual is—
(i) aged under 18, or
(ii) aged 18 or over and at risk,
(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and
(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are—
(a) in the circumstances, consent to the processing cannot be given by the data subject;
(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;
(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub- paragraph (1)(a).

(3) For the purposes of this paragraph, an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual—
(a) has needs for care and support,
(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and
(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it."

Part 3 Section 30: Protecting Individual's Vital Interests

"30 This condition is met if:
(a) the processing is necessary to protect the vital interests of an individual, and

(b) the data subject is physically or legally incapable of giving consent."

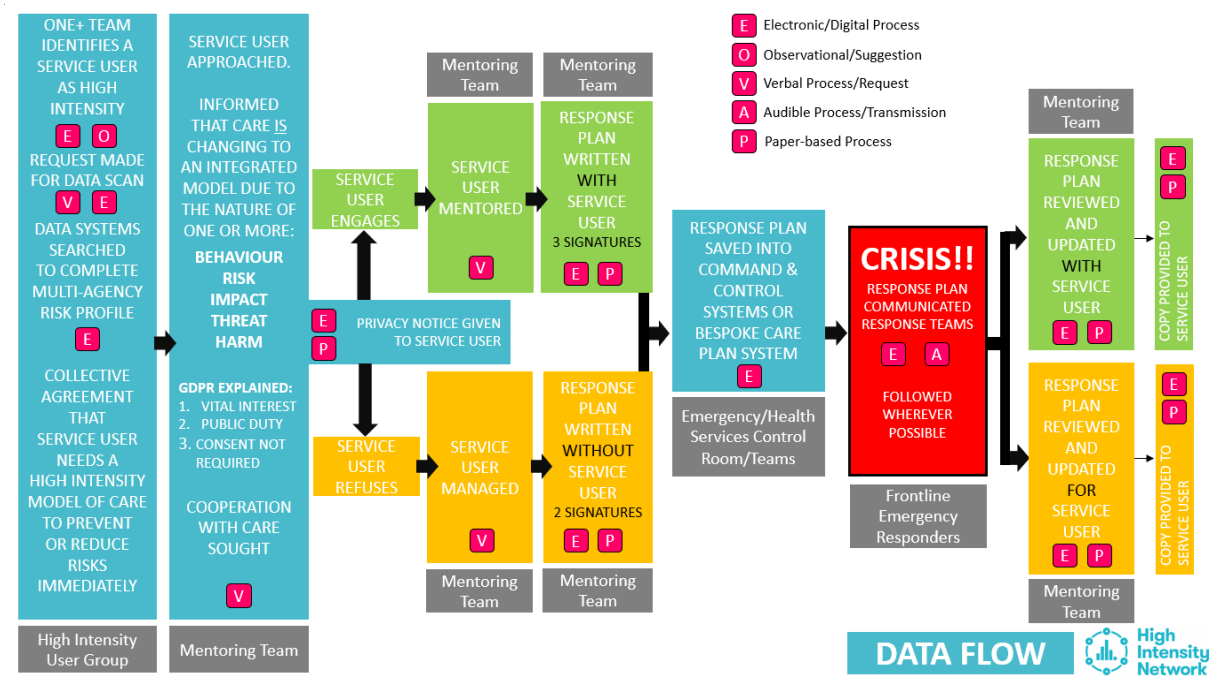
Finally, the **Health and Social Care Act 2012** provides that:

251B: Duty to share information

"(1) This section applies in relation to information about an individual that is held by a relevant health or adult social care commissioner or provider ("the relevant person").
(2) The relevant person must ensure that the information is disclosed to:
(a) persons working for the relevant person, and
(b) any other relevant health or adult social care commissioner or provider with whom the relevant person communicates about the individual, but this is subject to subsections (3) to (6).
(3) Subsection (2) applies only so far as the relevant person considers that the disclosure is:
(a) likely to facilitate the provision to the individual of health services or adult social care in England, and
(b) in the individual's best interests.
(4) The relevant person need not comply with subsection (2) if the relevant person reasonably considers that one or more of the following apply:
(a) the individual objects, or would be likely to object, to the disclosure of the information;
(b) the information concerns, or is connected with, the provision of health services or adult social care by an anonymous access provider;
(c) for any other reason the relevant person is not reasonably able, or should not be required, to comply with subsection (2)."

7. Information Flow

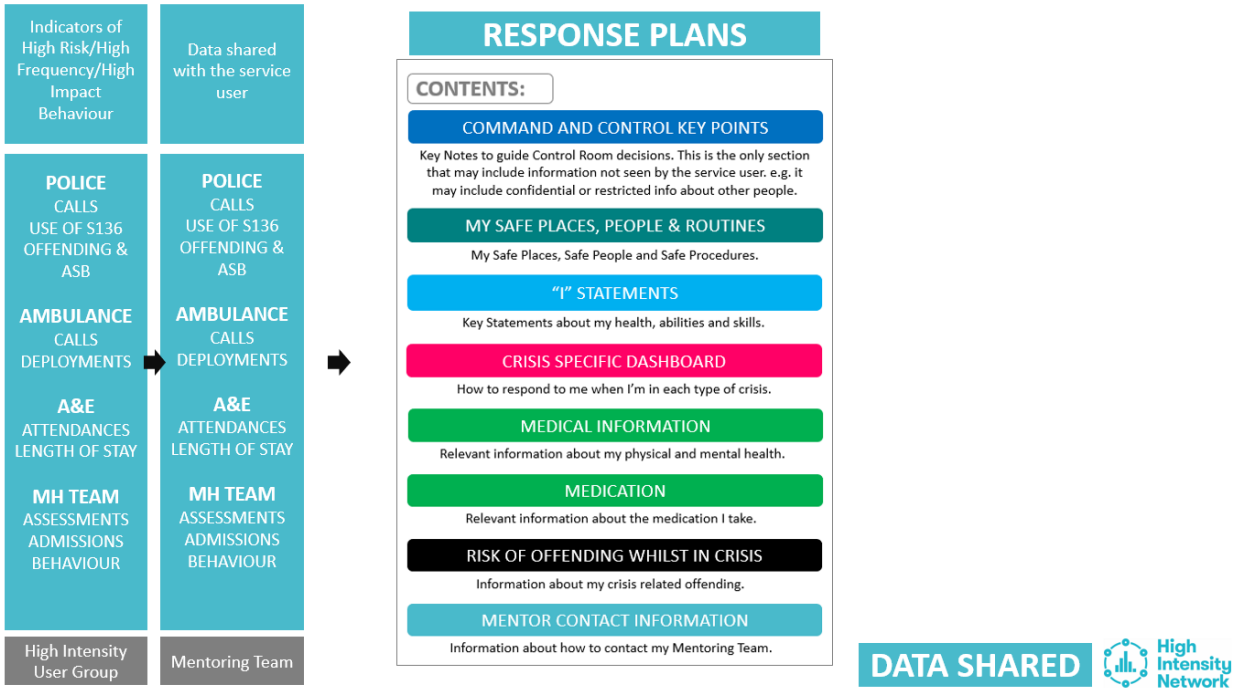
Please see **Document 5** for this **Data Flow Chart**, which details the process of information exchange and the format by which data maybe passed (e.g. electronically, verbally, audibly, paper document etc).



Secure routes of transfer (for instance CJSM, NHS.net mail, Egress Switch) will be used to transfer information between signatories.

8. Information Shared

Please see **Document 4** for this **Data Shared** chart, which details what information is assessed, shared or recorded at each stage of the data flow. The full response plan can be found in **Document 10**.



9. Data Controller(s)

Each public service team (NHS Trusts, Police Forces, Ambulance Trusts) hold the responsibility as Data Controller for the data they collect, record and store within their own system. They then provide data from their own systems as part of a High Intensity User Group which locally identifies and manages high risk behavioural service users.

Once identified, a service user will be supported by a High Intensity Team comprising a member of staff from the NHS Mental Health Trust and a member of staff from the Police Force. Together they will create a response plan for the service user. Ownership of these documents are shared by these two organisations.

Response Plan documents are then sent to the Ambulance Service and the Acute NHS Trusts that manage the local A&E departments who store copies of the plan (this can be both paper copies and electronic copies).

10. Data Quality

Personal information will only be collected using approved collection methods, ensuring the required information is complete and up-to-date. These methods are as follows:

1.

2.

3.

All reasonable steps must be taken to ensure that anyone who has received information is notified of any relevant changes and if any inaccuracies are found the necessary amendments will be made. This includes the data subject themselves if updates are made to their response plan.

11. Retention and Disposal

Personal information disclosed under this agreement will not be held for longer than necessary to fulfil the purpose for which it was collected and will be disposed of securely in accordance with national guidance, including the **Records Management Code of Practice for Health and Social Care 2016**, and each organisation's local information retention and disposal policy. Due to the enduring and life-long nature of the clinical conditions that cause high intensity behaviours, it is recommended that data be stored for as long as the law allows, to facilitate the provision of future support to the individuals in question.

12. Subject Access and Freedom of Information

Participating partner organisations acknowledge a duty to assist one another in meeting their individual responsibilities under the **GDPR 2018** and the **Freedom of Information Act 2000** to provide information subject to this agreement in response to formal requests.

Freedom of information requests should be directed to the relevant teams within each organisation. Specifically:

1) There should be consultation and cooperation between organisations as to responses to complaints and Subject Access Requests

2) There should be specific email addresses for each organisation to which data losses etc. should be reported (within specified time periods).

13. Breach of Agreement and Incident Reporting

Any breach of this agreement should be reported without undue delay and investigated in line with each partner organisation's incident reporting and management procedure and any relevant statutory guidance, including Articles 33 and 34 of the **GDPR 2018**.

14. Complaints

Each partner organisation has a formal procedure by which individuals can direct, their complaints regarding the application of this OA. Specifically:

1) There should be consultation and cooperation between organisations as to responses to complaints and Subject Access Requests

2) There should be specific email addresses for each organisation to which data losses etc. should be reported (within specified time periods).

15. Review

This OA will be subject to local approval and reviewed on the **31st March 2019** or sooner if appropriate.

16. Contacts

The primary contact for matters relating to the operation and management of this OA are:

Responsible Person		**Organisation**
Name:	X	X
Position:	X	
Name:	X	X
Position:	X	
Name:	X	X
Position:	X	
Name:	X	X
Position:	X	
Name:	X	X
Position:	X	

17. Authorised Signatories

In signing the document each signature is an undertaking to adopt the Agreement on behalf of their organisation

Name: .....

Role: ….....

NHS MENTAL HEALTH TRUST……..

Date: .....

Name: …….....

Role: …….....

POLICE ORGANISATION ……..

Date: .....

Name: …….....

Role: …….....

AMBULANCE ……..

Date: .....

Name: …….....

Role: …….....

ACUTE TRUST (A&E) ……..

Date: .....