Privacy Notice

How public services (and organisations working on their behalf), operating within the High Intensity Network, use and share sensitive and non-sensitive information concerning individuals whose mental ill health and/or behavioural disorders pose a high risk of death, serious injury, serious harm, community impact or criminality/anti-social behaviour.

Who we are

The High Intensity Network is made up of the following organisations:

[insert names based on local groupings]

The Data Protection Officers for these organisations can be contacted through:

[insert details]

The categories of information that we may process include:

- **Personal identifiers directly associated with crisis care** (such as name, date of birth, address, telephone numbers, NHS number, Police National Computer number, Police Force reference number, Ambulance reference number, ethnicity, appearance including marks, scars or tattoos).

- **Personal characteristics directly associated with crisis care** (such as ethnicity, nationality, language spoken, mannerisms, traits and habits).

- **Safeguarding information directly associated to crisis care** (such as behavioural risks from the individuals we work with or associates, risks to the data subject by known associates, character traits that make the data subject vulnerable, reasons why the data subject poses a risk to other people).

- **Disability and/or educational needs directly associated to crisis care** (such as physical disability/mobility, learning difficulties, communication difficulties, difficulties understanding or retaining information).

- **Medical information directly associated to crisis care** (such as diagnostic information relating to the individual's mental and physical ill health that may be important when deciding how to care for them in crisis).

- **Behavioural information directly associated to crisis care** (such as diagnostic information relating to the individual's personality traits or behavioural health that may be important when deciding how to care for them in crisis).

- **Criminal or police record information directly associated to crisis care** (such as the individual's behaviour in previous mental health crises that resulted in the commission of criminal offences, their arrest, caution, attendance at court or other formal or informal criminal justice disposal. Any behaviour or aggravating factors during crisis that may pose a risk to any persons present at a similar incident).

- **Contact information for friends/family/associates directly associated to crisis care** (such as names, addresses, telephone numbers or email addresses for people who are willing to care for the data subject when in crisis).

Why we collect, process and share the individual's information

We use the data subject's data to:

- Identify the individual as needing enhanced care.
- Perform multi-agency risk assessments about the individual.
- Prevent the death of, or serious injury to the individual.
- Prevent any other person being harmed by the behaviour of the individual.
- Prevent damage to property.
- Improve the quality of care provided by NHS mental health services.
- Improve the quality of response by police and ambulance personnel.
- Improve the quality of information provided to 999 response staff when making key decisions about how a crisis incident will be managed and concluded, including any use of police powers (such as s136 of the Mental Health Act 1983).
- Ensure that the criminal justice system is used where lawful, proportionate, necessary and is in the public interest.
- Reduce unnecessary, inappropriate, anti-social or avoidable demands placed on public services.
- Use elements of information (in anonymised formats) as part of national research programmes into high intensity crisis care, so that we can continuously improve.
- Support the high intensity team supporting the data subject with clinical advice.

How do we share data?

We usually first discuss a newly referred patient at a face to face, multi-agency panel which sits once a month, specifically to discuss individuals who are frequently using emergency and healthcare services. If organisations present, have information that relates to the risk assessment process, then they share this information.

If an individual is felt suitable to be managed by a high intensity team, then information sharing processes become more reactive and dynamic from this point on. Additional information can be shared face to face or via secure electronic communication or in writing.

Only information that is necessary and proportionate to the task at hand is shared.

What law allows the sharing of data?

The **General Data Protection Regulation (GDPR)** became law on **May 25th, 2018**.

Article 6 of the GDPR provides several **lawful bases** that can be relied on for processing personal information. Two of these apply in particular, to processing and sharing information about high intensity users of services. They are:

Article 6 (1)

(c) processing is necessary, to **protect the vital interests** of the individual or of another person.

Working in the vital interests of the service user include taking pro-active steps to prevent incidents, events or circumstances where the likelihood of death or serious harm to the data subject increases. Such work can be conducted:

- *To protect the vital interests of an individual when they are in crisis*
- *To protect the vital interests of an individual by preventing future crises*

(d) 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.

Such tasks and authorities include:

- *To prevent crime and disorder and prevent a breach of the peace*
- *To protect property*
- *To safeguard vulnerable people*
- *To prevent death, improve quality of life and provide the highest possible standards of clinical care*
- *To provide public services as effectively and efficiently as possible, reducing where possible demands upon services that are unnecessary, inappropriate or avoidable*
- *To provide services as cost effectively as possible*

Accordingly, we do not rely on an individual's 'consent' to process information about them as part of the HIN programme but we do work closely and actively with individuals who participate in the programme.

What are 'special categories' of data and can they be shared?

Article 9 of the GDPR explains how organisations can (in certain circumstances) share special categories of data when necessary. Special category data includes more sensitive information about a data subject, including their race or ethnicity, their sexual orientation, their religious beliefs or their biometric or genetic data. Because organisations providing care for high intensity individuals can rely on Article 6(1)(c) and (d) to process and share data, it also means that they can share special category data, BUT they must only do so if it is **honestly believed** to be **necessary and proportionate** to the circumstances or risks.

Below are some examples of where sharing special category information maybe important.
Please note: We have made these examples up and used random names:

Example 1: ***THIS CASE IS NOT REAL – WE HAVE CREATED IT PURELY TO PROVIDE AN EXAMPLE***
Sonya regularly self-harms because of the guilt she feels from becoming pregnant as a single mum. Her guilt comes from the relationship she has with her parents who have recently disowned her. Her family are members of a local religious brethren whose culture is to expel any person who commits any sexual sin.
It is felt important for professionals to share details about Sonya's religious beliefs so that the best care and support can be provided.

Example 2: ***THIS CASE IS NOT REAL – WE HAVE CREATED IT PURELY TO PROVIDE AN EXAMPLE***
Henrietta is 19-years old who has a diagnosis of Emotionally Unstable Personality Disorder. Her difficulties in regulating her emotions are usually triggered by her feelings of isolation amongst her friends and family. Henrietta was born a boy and still is biologically male. She wants to undergo gender re-assignment surgery but is highly anxious about what people will think. Sometimes she wishes she was dead.
It is felt important for professionals to share details about Henrietta's struggle with her sexual identity so that the best care and support can be provided.

Example 3: ***THIS CASE IS NOT REAL – WE HAVE CREATED IT PURELY TO PROVIDE AN EXAMPLE***
James is being managed by a high intensity team but has recently fallen out with his mentors as they have imposed some new rules about what services he can and can't ask for when in crisis. So, he has started to get on trains and buses so that he can have a crisis in another area where he isn't known. He has also started to climb off bridges onto railway lines (which is a criminal offence) and he has also started to provide false identities, so he isn't recognised or arrested again.
James' team have contacted all neighbouring forces and NHS trusts to warn them about his escalating behaviours. This includes information about how to identify him (Marks, scars, tattoos and his DNA reference number). A flag has also been placed on his PNC (Police National Computer) record.

How is data stored?

We hold data securely for the set amount of time shown in our data retention schedules. For more information, contact the Information Teams within each individual organisation.

Which organisations share information and how often do they do this?

Routine sharing of data about an individual is likely to be conducted locally by a multi-agency management group (usually called a *High Intensity User Group*), comprising of NHS Mental Health staff, Police mental health leaders, Ambulance Service representatives and A&E representatives. Some of these staff maybe specifically employed to manage individuals who have a history of repeatedly demanding services. Such groups may also have other organisations present who are contracted to work for the NHS, such as specialist charity and 3rd sector organisations.

Can organisations share data across geographical borders within the UK? Does my data go anywhere else?

Yes. Should the data subject experience a crisis outside of the geographical area in which they usually reside, information can be shared across NHS, Policing and Ambulance organisations. To consistently identify the data subject, information that assists 'out of area' staff and directs them to care and response plans are often placed on national record systems such as the Police National Computer. Work is currently underway to develop a national mental health response plan system accessible by all 60 mental health trusts, all 43 police forces and all 10 ambulance trusts across England and Wales.

We do not, however, send data overseas.

How long is data kept for?

Records are held by members of the High Intensity Network in accordance with their respective record keeping policies, and this may be longer than your active involvement with the High Intensity Network programme, because records need to be kept for clinical and governance purposes.

Do you make decisions about people automatically?

No. Professionals will work together to make effective multi-agency decisions to seek to achieve the targets of the HIN programme, and as far as possible the individual him or herself will be involved in those decisions.

What education and training do staff have about information sharing?

All staff who work with individuals being managed by high intensity teams attend a 3 day initial classroom-based course and then complete online courses too. Modules within both courses teach them about their duties and responsibilities to share information where lawful, proportionate and necessary.

Can I request access to personal data?

Yes. Under data protection legislation, the data subject (or a person acting on their behalf) will be able to request information about them held by each organisation. To make a request for your personal information, contact the Information Teams within each individual organisation.

Is there a right to object/complain?

Yes. The data subject (or a person acting on his/her behalf) has the right to:

- *Object to the processing of personal data that is likely to cause, or is causing, damage or distress.*
- *Prevent processing for direct marketing*
- *Object to decisions being taken by automated means*
- *In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and*
- *A right to seek redress, either through the ICO, or through the courts*

In certain circumstances, organisations may not be able or required to comply with these requests, but will clearly explain the reasons for refusal. Unresolved concerns should be made to the **Information Commissioner's Office** at https://ico.org.uk/concerns/

For more information:

For more information on the General Data Protection Regulation: https://ico.org.uk/your-data-matters/

If you would like to discuss anything in this privacy notice, please contact your local NHS/Police team or the High Intensity Network. www.highintensitynetwork.org