NHS England

Practical Guidance on the sharing of information and information governance for all NHS organisations specifically for Prevent and the Channel process

NHS England Information Reader Box

Directorate

Nursing

Publication Gateway Reference: 06915

Document Purpose	Guidance
Document Name	Practical Guidance on the sharing of Information and Information Governance for all NHS organisations specifically for Prevent and the Channel Process.
Author	NHS England Prevent Team
Publication Date	July 2017
Target Audience	All NHS employees
Additional Circulation List	
Description	Guidance to strengthen the information sharing and information governance regarding Prevent
Cross Reference	
Superseded Docs (if applicable)	
Action Required	
Timing / Deadlines (if applicable)	
Contact Details for further information	Prevent Team Nursing Directorate 3 Leeds City Office Park Meadow Lane Leeds LS11 5BD

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

Practical Guidance on the sharing of Information and Information Governance for all NHS organisations specifically for Prevent and the Channel Process

Version number: 3

First published: March 2017

Updated: June 2017

Prepared by: NHS England

Classification: OFFICIAL

Contents

1 Executive Summary

1.1 This guidance is intended to assist those involved in Information Sharing and Information Governance for the purpose of Prevent. It is designed to assist in the decision making process about the appropriateness of sharing information (particularly sensitive health information) such as the decisions made by Caldicott Guardians.

1.2 There are already a number of documents to inform and guide staff in their decision making process when considering the sharing of personal information. This document provides a brief overview of the key principles that are particularly relevant to Prevent, and to highlight in the attached Appendices, the particular sections of legislation and guidance that may be relevant.

1.3 The guidance has been developed in response to concerns raised by health care practitioners about information sharing for the purposes of Prevent and Channel particularly when:

- They are requested to share information without the individuals' prior consent or
- The individual has not been explicitly identified as being at risk of harm, abuse or exploitation

1.4 The aim is to support practitioners to be confident in their actions and to understand how they can share information appropriately, proportionately and lawfully.

1.5 Effective information sharing is the key to the delivery of Prevent, enabling partners to take appropriate, informed action and is central to providing the best support to those who are vulnerable to radicalisation. This is particularly the case for objective 2 of the Prevent Strategy, 'protecting vulnerable people, who may be drawn into terrorism ensuring that they are given appropriate advice and support'. (Appendix 1)

1.6 Everyone who works within the NHS or is a healthcare provider in England (including staff, contractors and volunteers) has a duty of confidentiality and a responsibility to safeguard any NHS England information or data that they access.

2. Key Principles

2.1 The sharing of personal or sensitive personal data needs to be considered carefully, particularly if consent from the individual is not to be sought or obtained. It is considered to be good practice to have an Information Sharing Agreement [ISA] in place at a local level to support this process, this is considered to be best practice. A link to an example of an ISA is included later in this document. (Appendix 1)

2.2 It is important that this agreement is signed by the appropriate senior level member of staff, (usually the Caldicott Guardian) for each NHS organisation.

2.3 Necessary and Proportionate

2.4 When considering sharing of data there is a need to consider whether it is necessary and proportionate to share the information when the risk to both the individual and/or the public is considered.

2.5 When considering sharing personal data with relevant authorities, you will need to consider:

- Why are you sharing? – the purpose and the legal basis for sharing the information.
- What are you intending to share – is it relevant and proportionate for the purpose of the sharing?
- With whom – do they really need it? Do they have a lawful basis to request or to have this information?
- Consent – have you gained the consent of the data subject, or if consent has not been gained, or sought, what other legal basis are you using for disclosing the data?

2.6 Consent

2.7 Consent should be obtained wherever possible. If it is not obtained, or if consent is withheld, you will need to satisfy another lawful basis to share the information.

Decision making should comply with all of the following:

- Data Protection Act (DPA) 1998; (Appendix 1)
- Common Law Duty of Confidentiality (if you are looking to share sensitive personal data); (Appendix 1)
- Human Rights Act (HRA). (Appendix 1)

2.8 Compliance with the DPA and HRA are significantly simplified by having the subject's consent. Consent must be informed and unambiguous particularly in the case of sensitive personal information; the individual should understand how and

for what purpose their information will be used. If consent is received this should be recorded.

2.9 There will be circumstances of course, when seeking the consent of the individual will not be desirable or possible because it will prejudice delivery of the intended outcome, or may increase the risk of significant harm to the individual or the public.

2.10 In these circumstances there are gateways or exemptions which permit sharing of information to take place without consent, if for example, it is required by law or can be justified in the public interest.

2.11 The Power to Share

2.12 Public bodies are required to meet the requirements of the DPA, HRA and Common Law Duty of Confidentiality (CLDC). Some statutes confer a permissive or mandatory gateway to sharing information for particular purposes; such as section 115 of the Crime and Disorder Act 1998. (Appendix 1:6)

2.13 A permissive gateway means you may consider sharing information to help prevent or detect a crime, however, you can however still refuse to share information.

2.14 Whereas a mandatory gateway means you must share the information specified or requested, it imposes a legal obligation on public bodies to provide relevant information.

2.15 CLDC arises in situations where an individual provides sensitive information about themselves, in the expectation that the person they are disclosing to will keep that information confidential (e.g.: doctor/patient relationship). Meeting this requirement can be done by:

- Getting consent of the individual to share for a particular purpose;
- Statutory disclosure is required (e.g. Court Order);
- The public interest in disclosure outweighs the duty of confidence owed to the individual. Disclosure in the public interest needs to be documented and justified, be made using a balance of judgements, and used on a case-by-case basis. Disclosures made in the public interest should not be used on a routine basis.

2.16 It will also be necessary to ensure compliance with the DPA by (in all cases) either by meeting the processing conditions in Schedules 2 and 3 (if sensitive personal data is to be shared). Or by relying on one of the exemptions [such as section 29 for the prevention of crime].

2.17 Exemptions

2.18 The DPA contains exemptions for how data is used. They do not exempt the Data Controller from all parts of the DPA, only from certain parts (as specified in each exemption).

2.19 The main section for the police is the s29 exemption. This exemption allows the police to approach a Data Controller with an exemption to the DPA for the purpose of detecting or preventing a crime.

2.20 The Data Controller is exempt from telling data subjects they have shared any records/documents with the police, as long as the purpose for the disclosure is for the prevention or detection of crime or apprehension of offenders and to do so would prejudice the cause [investigation].

2.21 **You will need to be certain that there is justification for not informing the data subject, a log of the decision making process should be maintained.**

2.22 Section 29 would not automatically 'switch off' the data subject's right to be informed of the disclosure, this should be considered on a **case by case** basis as whilst it is likely that informing the data subject might be detrimental to an investigation, there should be no automatic assumption of this.

2.23 It would be advisable to **seek advice** and approval from the Caldicott Guardian in such matters. A record must be kept as part of a Caldicott log.

2.24 Section 29 also allows a Data Controller to proactively disclose information to the police, as long as the purpose is for the prevention/detection of crime, or the apprehending of offenders. The Data Controller in this case, is exempt from Principles 1-5 DPA 1998, section 10 (right to object to processing) and section 14 (right to altering, rectification, destruction etc. by court order).

2.25 The Data Controller will still need Caldicott approval for such a disclosure, and the same considerations apply as mentioned in s2.19 of this document which refers to justifying and logging any decision not to inform the data subject via Caldicott guardian approval

2.26 **You may need to consider how the request for information is made; this may be by the use of an agreed document:**

- Crime and Disorder Act –section 29, prevention of crime; The police typically use their own S29 forms (DP7 – non-consented disclosures and DP9 where they have the subjects consent)
- Data Protection [processing of sensitive personal data] Order 2000,[SI 2000/417] - of particular relevance to Prevent is paragraph 1 [purpose of the prevention or detection of crime] and paragraph 4[discharge of any function designed to provide confidential counselling, advice, support or other service].
- If you are sharing with non-public bodies you should be confident that they are aware of their own responsibilities under the DPA.

2.27 Legislation and guidance relevant to information sharing

2.28 Although not an exhaustive list, the following acts and statutory instruments may be relevant. The original legislation can be found at the Statute Law Database or type into your browser http://www.legislation.gov.uk/**.**

2.29 Data protection

2.30 Data Protection Act (DPA) 1998

2.31 The DPA is the principal legislation governing the use and processing (including collection, storage and disclosure) of data relating to individuals. The Act defines:

- personal data (as information by which an individual can be identified ether on its own or with other information);
- sensitive personal data (including information about an individual's health, criminal record, and political or religious views);
- the circumstances in and extent to which they can be processed details the rights of data subjects.

2.32 All of the eight data protection principles (which are listed in part 1 of schedule 1 to the Act) must be complied with when sharing personal data but the first data protection principle is particularly relevant. The first data protection principle states that personal data shall be processed:

- **Fairly;** this requirement for fair processing will not be met if the data subject is not informed about that processing, without good reason for not doing so.

- **Lawfully** (meaning that there is the power to share and other statutory and common law obligations must be complied with), and only if a condition in schedule 2 and, if sensitive personal data is involved, schedule 3 is met.

2.33 Both of these requirements must be met to comply with the first data protection principle. The DPA cannot render lawful any processing which would otherwise be unlawful.

2.34 If compliance with the data protection principles is not possible, then one of the exemptions (such as the prevention of crime under section 29 of the Data Protection Act 1998) may apply, which may exempt you from some of the Principles.

2.35 Data Protection (Processing of Sensitive Person Data (Appendix A) Order 2000

2.36 This Statutory Instrument (SI 2000/417) specifies further conditions under which sensitive personal information can be processed, including conditions where the processing must necessarily be carried out without the explicit consent of the data subject.

2.37 Of particular relevance to Prevent are paragraph 1 (for the purposes of prevention or detection of crime), and paragraph 4 (for the discharge of any function which is designed for the provision of confidential counselling, advice, support or any other

service).

2.38 The first data principle states that personal data shall be processed fairly and lawfully, meaning that other statutory and common law obligations must be complied with, and that the DPA cannot render lawful any processing which would otherwise be unlawful. Schedules 2 and 3 of the Act provide the conditions necessary to fulfil the requirements of the first principle.

2.39 Human Rights Act (HRA 1998)

2.40 Article 8 of the European Convention on Human Rights has particular relevance to Prevent. It states that individuals have a right to respect for private and family life. The HRA further states that:

2.41 “Everyone has the right to respect for his private and family life, his home and his correspondence”, and that public authorities shall not interfere with “the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.

2.42 Common Law Duty of Confidentiality (CLDC)

2.43 CLDC is built up from case law and its basis is that information that has the necessary quality of confidence should not be used or disclosed further, except as originally understood by the discloser, or with their subsequent permission. Some situations and relationships (such as Doctor/Patient relationship) also add a level of quality to the information imparted, which can help to achieve the necessary threshold for CLDC. Case law has been established that exceptions can exist “in the public interest”; and confidentiality can also be overridden, or set aside, by legislation.

2.44 The Department of Health [DH] has produced a code of practice concerning confidentiality, which is required practice for those working within or under contract to NHS organisations. DH – Code of Practice on protecting the Confidentiality of service user information [Jan 2012. chapters 3 and 5]. (Appendix 1).

2.45 Gateways, exemptions and explicit powers

2.46 **Crime and Disorder Act (CDA) 1998**

2.47 Section 115 confers a power to disclose information to a “relevant authority” on any person who would not otherwise have such a power, where the disclosure is necessary or expedient for the purposes of any provision of the Act.

2.48 The “relevant authority” includes a chief officer of police in England, Wales or Scotland, a police authority, a local authority, a health authority, a social landlord or a probation board in England and Wales. It also includes an individual acting on behalf of the relevant authority. The purposes of the CDA include, under

section 17, a duty for the relevant authorities to do all that they reasonably can to prevent crime and disorder in their area.

2.49 **Common Law Powers**

2.50 Because the range of partners, with whom the police deal has grown – including the public, private and voluntary sectors, there may not be either an implied or explicit statutory power to share information in every circumstance. This does not necessarily mean that police cannot share the information, because it is often possible to use the common law. The decision to share using common law will be based on establishing a policing purpose for the activity that the information sharing will support, as well as an assessment of any risk.

2.51 **The Code of Practice on the Management of Police Information (MoPI)**

2.52 The Code of Practice on the Management of Police Information (MoPI) defines policing purposes as: protecting life and property, preserving order, preventing the commission of offences, bringing offenders to justice, and any duty or responsibility of the police arising from common or statute law. (Appendix 1)

2.53 **Local Government Act 1972**

2.54 Section 111 provides for local authorities to have “power to do anything…which is calculated to facilitate, or is conducive or incidental to, the discharge of any of their functions”.

2.55 **Local Government Act 2000 (Appendix A – Section 2(1))**

2.56 Local Government Act 2000 (Appendix A – Section 2(1)) provides that every local authority shall have the power to do anything which they consider is likely to achieve the promotion or improvement of the economic, social or environmental wellbeing of the area.

2.57 National Health Service Act (NHSA) 2006 Section 251 of the NHSA 2006 provides a power for the Secretary of State to make regulations governing the processing of patient information.

2.58 **Offender Management Act (OMA) 2007**

2.59 Section 14 of the OMA enables disclosure of information to or from providers of probation services, by or to Government departments, local authorities, Youth Justice Board, Parole Board, chief officers of police and relevant contractors, where the disclosure is for the probation purposes (as defined in section 1 of the Act) or other purposes connected with the management of offenders.

Appendix 1 – Further reading

Documents are available in support of this guidance and have been referenced throughout .This guidance should therefore be read in conjunction with the following documents:

1. Prevent Duty 2015
https://www.gov.uk/government/publications/prevent-duty-guidance

2. Example Information Sharing Document [ISA]
www.this.nhs.uk/fileadmin/IG/interagency-information-sharing-protocol.pdf

3. Data Protection Act [DPA] 1998 –Paragraph 1 is of particular relevance to Prevent.
https://www.gov.uk/data-protection/the-data-protection-act

4. Common Law Duty of Confidentiality
https://www.health-ni.gov.uk/articles/common-law-duty-confidentiality

5. Human Rights Act [HRA] 1998 – Schedule 1 part 1 article 8
www.legislation.gov.uk

6. Information Commissioner's Office Guidance on Interpretation of the DPA
https://ico.org.uk/for-organisations/guide-to-data-protection/

7. Department of Health[DOH] – Code of Practice on protecting the confidentiality of service user information Jan 12 p43, ch5
https://www.health-ni.gov.uk/publications/dhssps-code-practice-protecting-confidentiality-service-user-information

8. Crime and Disorder Act 1998 – section 29 prevention of crime – section 115
http://www.legislation.gov.uk/uksi/2000/417/made

9. Management of Police Information .[MOPI]
https://ict.police.uk

10. Channel Duty Guidance
https://www.gov.uk/government/publications/channel-guidance

11. Caldicott and Caldicott 2
https://www.gov.uk/government/publications/the-information-governance-review

12. NHS Confidentiality Code of Practice (Privacy Impact Assessment – P27 1st paragraph)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf

13. Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers
https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice

14. European Convention on Human Rights
http://rightsinfo.org/the-rights-in-the-european-convention

15. NHS-wide Code of Practice and supplementary guidance on public interest disclosures
https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

Appendix 2 – Key messages

All IG/ Information sharing agreements that are signed on behalf of the organisation should have specific reference to Prevent.
All safeguarding policies should reference Prevent.
If you are a Channel Panel member and are asked to sign an explicit and specific confidentiality agreement for the purposes of Channel you should ensure that your organisational Caldicott or Data Controller is sighted on the document.
All staff should be aware of who their organisational Data Controller is and how to contact them as they are responsible for giving guidance within an organisation.
Consideration should be given as to how staff, particularly Prevent Leads, are made aware of the process and legal position for sharing information legally.
In line with information sharing policy there should be clarity as to what basis the information is being shared, is it being shared for safeguarding purposes or national security or the prevention of crime.

Get in touch

Email - england.safeguarding@nhs.net
NHS England
Quarry House, Quarry Hill, Leeds, LS2 7UE
Twitter - @NHSENGLAND