Department of Health & Social Care

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

Table of Contents

1. Introduction

This guidance is intended to assist those involved in information sharing and information governance for the purposes of safeguarding individuals from radicalisation under the Prevent programme.

This document provides a brief overview of the key principles that are particularly relevant to Prevent (but which are also common to other safeguarding principles). Prevent is no different to any other safeguarding risk, and the same rigour is applied to information sharing in this context as to any other concern relating to personal harm.

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

- They are making an initial Prevent referral regarding a vulnerable individual who may be at risk of being radicalised or drawn into terrorism, or
- They are requested to share information for Prevent purposes with partner agencies, including the police and local authority, with or without the Data Subject's prior consent.

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

Effective information sharing is 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 being drawn into terrorism.

This is particularly the case for the first objective of the UK government's CONTEST strategy; "Safeguarding and supporting those at most risk of radicalisation through early intervention, identifying them and offering support" (see Appendix 1: Further Reading).

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 personal or patient data that they access.

Timely and effective information sharing is a key element of Prevent, as with all other safeguarding concerns. It is therefore vital that healthcare organisations are familiar with their organisational policies and procedures on information sharing and have arrangements in place so that information can be shared with partners when necessary for Prevent purposes. This should include clear guidance as to how Prevent concerns are noted on patient records and handed over when patients are transferred.

Executive Summary

- When considering the sharing of personal data, there is a need to decide whether it is necessary, proportionate and lawful to share this information when the risk to both the individual and/or the public is considered.

- Any disclosures or discussions on sharing personal data or consent must always be documented in an appropriate location in the patient record.

- In line with information sharing policy, there should be clarity as to what legal basis the personal data is being shared with and processed by other third parties, and whether it's being shared for safeguarding purposes, national security or the prevention of crime.

- Confidentiality is an important ethical and legal duty, but it is not an absolute and can be overridden without breaching duties of patient or staff confidentiality if the disclosure is for safeguarding or public interest reasons and where the public interest test can be met.

- There are legal exemptions contained in the Data Protection Act 2018 (DPA 2018) which allow for information sharing to take place in this context. The General Data Protection Regulation (GDPR) (Article 6 (e)) allows for the lawful processing of personal data "*where it necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"*. Further details from the Information Commissioner's Office (ICO) about how to judge if the public interest test is met can be found on the ICO website[1].

- The third party (i.e. police or local authority) must always define a legitimate purpose or public interest for the receipt and processing of personal data.

- All organisational safeguarding policies should reference Prevent.

- All Data Sharing Agreements that are signed on behalf of the organisation should have specific reference to Prevent.

- All staff should be aware of who their organisational Information Governance Team/Data Protection Officer and Caldicott Guardian are and how to contact them, as they are responsible for providing advice on the legal or ethical justification for sharing personal data.

- Consideration should be given as to how staff, particularly Prevent/Safeguarding Leads, are made aware of the process for sharing personal data within the prescribed legal frameworks as described in this document.

- If you are a Channel Panel member and are asked to sign a purpose-specific Channel data sharing agreement, then you should ensure that your Senior

[1] https://ico.org.uk/media/1183/the_public_interest_test.pdf

Information Risk Owner and/or organisational Information Governance team are sighted on the document and are able to provide appropriate advice.

- Every health practitioner has a duty and must take responsibility for sharing the information that they hold regarding Prevent safeguarding concerns and should not assume that someone else will pass on this information, which may be critical in keeping someone at risk safe.

2. Necessary, Proportionate and Lawful to Share Information

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

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

- **Why** are you sharing personal data? – the purpose and the legal basis for sharing the information.
- **What** are you intending to share? Is it relevant and proportionate and necessary for the purpose of the sharing?
- **With whom** – do they really need it? Do they have a lawful basis to request or process 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?

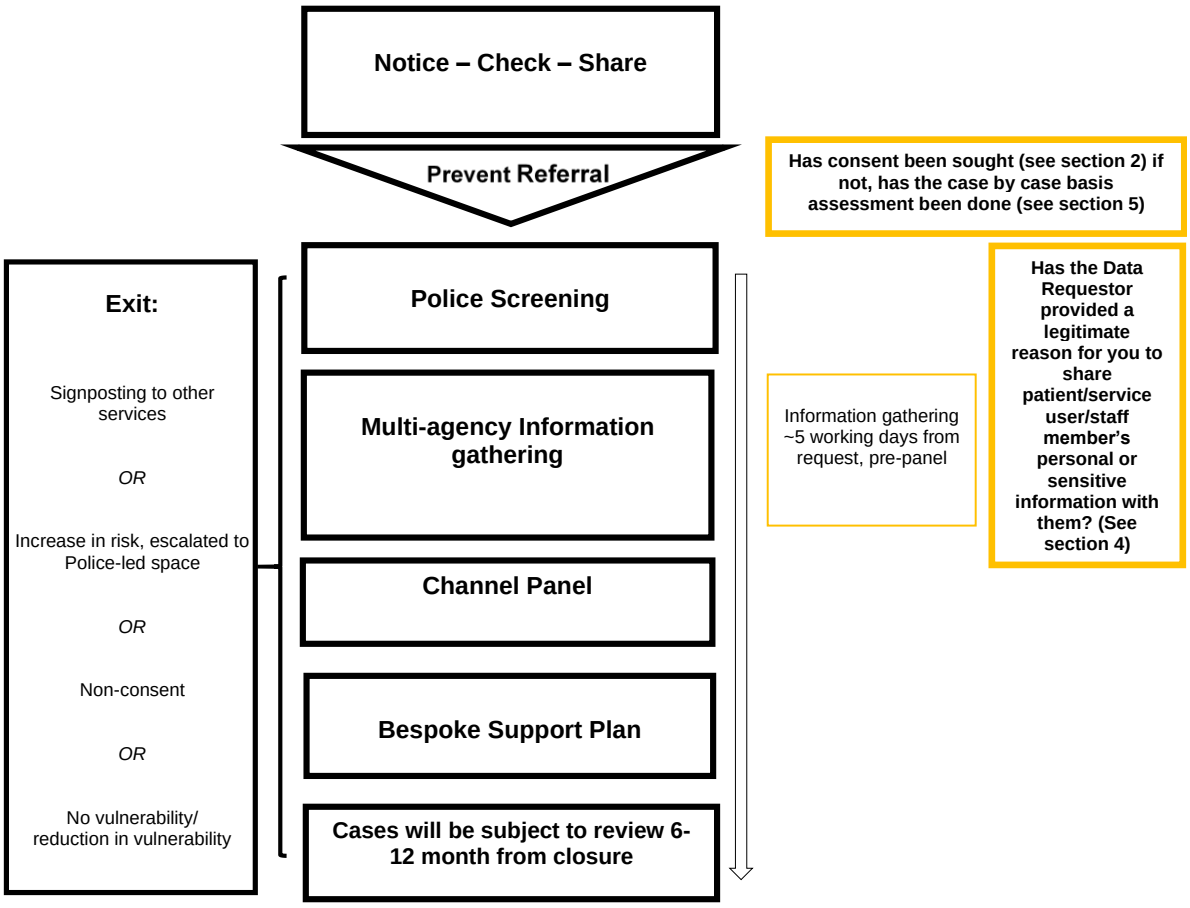
  There are occasions when it may not be inappropriate to seek consent from Data Subjects before sharing any records/documents with the police or other partners, particularly if the disclosure is for a legitimate safeguarding purpose, such as the prevention or detection of crime and for reasons of substantial public interest, and when informing the Data Subject would prejudice the intended outcome or lead to harm. (See Section 8: Legal gateways, exemptions and explicit powers and Section 3: Consent).

2.3 It may be advisable to seek advice and approval from your organisational Information Governance Team/Data Protection Officer or Caldicott Guardian in such matters, particularly if there is any doubt, a record of which must be kept as part of a Caldicott log.

3. Consent

3.1 The Prevent programme is designed to help prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support, including through the multi-agency Channel programme. See Diagram 1.0 below of Prevent and Channel pathways and Section 7: Channel and other partners.

Diagram 1.0: Prevent and Channel referral pathway



3.2 The health sector needs to ensure that the crucial trust-based relationship between patients and clinicians is balanced with the professional duty of care and their responsibility to safeguard and protect their patients and the wider public from harm.

3.3 **Although consent to share personal data is always the gold standard and must always be the preferred option for clinical staff and safeguarding leads, there are times when it is essential to share personal information to safeguard individuals or others from harm, and where it is appropriate to do so without patient consent.**

3.4 The DPA 2018 and GDPR has strengthened the need to demonstrate that consent is given freely to share someone's personal data or information and data controllers need to define a clarity of purpose for sharing/processing data with third parties (for further information please see **ICO Guidance on consent**[2]). Importantly, the legislation also ensures that criminal justice agencies and other statutory partners can continue to process and share personal data/special category data to prevent and investigate crime, bring offenders to justice, to safeguard the vulnerable and to

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

keep communities safe from harm (sometimes referred to as being the public interest).

3.5 The primary conditions for disclosing personal or special category data about staff members, patients or service users for the purposes of Prevent should always be based on the principle of informed consent. However, this may not always be appropriate or achievable, particularly within a safeguarding context.

3.6 If consent is not appropriate or achievable, then a different lawful basis must be met in order to share personal/special category data (see Section 8: Legal gateways, exemptions and explicit powers). These exemptions exist to facilitate the sharing of personal/special category data without consent for safeguarding and public interest reasons. However, exemptions should not routinely be relied upon or applied in a blanket fashion.

3.7 The General Medical Council (GMC) website contains a useful *Confidentiality Decision Tool*[3] to help with your decision-making regarding consent.

3.8 Best Interest Decisions

3.8.1 In cases where the vulnerable person lacks the capacity to give their informed consent (as described in the Mental Capacity Act 2005[4], parts 2-4) a referral may be made in certain circumstances without consent, in the Data Subject's best interests and in accordance with the five statutory principles as defined in Section 1 of the Act (also see HMG Mental Capacity Act 2005: Code of Practice).

3.8.2 Your decision and rationale should be clearly documented and recorded. **Please note**: Public interest and best interest decisions are described in greater detail in the GMC guidance document *Confidentiality: good practice in handling patient information*[5].

3.9 Disclosure required or permitted by law

3.9.1 There may in some circumstances be a legal requirement or a court order which compel clinicians or other staff to disclose patient sensitive data.

3.9.2 Care should always be taken to only disclose the information required to comply with and fulfil the purpose of the law. If you have any concerns regarding the disclosure, you should seek appropriate advice.

3.9.3 If in any doubt, or if you have any concerns about sharing personal or sensitive information in these circumstances, consult with your organisational Information Governance Team, Data Protection Officer, Legal Advisor and/or Caldicott Guardian for further advice and guidance.

4. Making a Prevent Referral

[3] https://www.gmc-uk.org/ethical-guidance/learning-materials/confidentiality-decision-tool
[4] https://www.legislation.gov.uk/ukpga/2005/9/contents
[5] https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality.

4.1 It is a key NHS safeguarding requirement for staff to know who to contact and where to seek advice if they have concerns about an individual who may be being groomed into terrorist activity and be able to raise concerns and take action when they arise.

4.2 All concerns should initially be discussed with the care team supporting the person prior to referral and your line manager. If agreed that escalation is appropriate, a conversation should be always be held with the organisational named Safeguarding Lead who is the gatekeeper for all Prevent referrals.

4.3 Organisations should have formal arrangements in place so that relevant and timely information can be shared with partners, for example local authorities or police, when necessary. It is regarded as good practice to have a data sharing agreement in place for safeguarding purposes.

4.4 This includes understanding the organisational Prevent referral pathway and having robust data sharing arrangements and formal referral pathways so that partners can be appropriately advised in a timely manner.

4.5 When making a Prevent referral to third party/partner agencies, including the police and local authorities, please consider all the following:

- You should use the standard **National Prevent Referral Form** to make the referral to your relevant police contact and the relevant Local Authority Prevent Coordinator using secure email i.e. via your secure NHS.net account.

- You should include contact details in the National Prevent Referral Form detailing where possible the original source/person who made the initial referral within your organisation. This will ensure that that the referral source can be contacted where necessary by police and relevant partner agencies if any further clarity is required.

- The form should be always be protectively marked at OFFICIAL SENSITIVE according to the Government Security Classification Policy[6] (see Section 9: Other relevant legislation/principles).

- If it has been decided that seeking consent from the patient/service user/staff member being referred is not appropriate, you should always clearly document your decision and rationale in the patient/service user/staff record (see Section 3: Consent). This should explain which public interest/ safeguarding and best interest considerations have been applied to set aside their rights under the Common Law Duty of Confidentiality (CLDC), the DPA 2018 or the Human Rights Act 1998 (HRA 1988) to safeguard and prevent harm.

4.6 The decision and rationale for making a referral without the Data Subject's informed consent should be subjected to a case-case basis assessment which considers whether the informed consent of the individual can be obtained, and if the proposed data sharing is legitimate, necessary, proportionate and lawful (see Section 6: Case-by-case decisions). This assessment should be based on your professional opinion

[6] https://www.gov.uk/government/publications/government-security-classifications

that there is tangible public interest or best interest considerations involved (i.e. you believe the individual may be of hard to themselves or others, and patient consent should therefore legitimately be overridden in this instance)

4.7 **Without the case-by-case assessment, there is a higher risk of unlawful sharing of personal data and there may be no legal basis to share personal data between statutory agencies (even for safeguarding purposes), without Data Subject's informed consent.**

5. Responding to Data Requests from Other Partners

5.1 When externals partners (third parties) request patient/staff information from health providers for Prevent case management purposes, you should always consider the following:

- Has the Data Requestor used an appropriate official information sharing request proforma sanctioned by their organisation? Different organisations have different forms for sharing personal data/special category data, and they should always be sent by secure email such as the police pnn.police.uk or Criminal Justice Secure Mail (CJSM) mail which is used by many local authorities. The email should always be protectively marked at OFFICIAL SENSITIVE according to the Government Security Classification Policy.
- Has the Data Requestor provided clarification on whether or not the Data Subject has consented to share or process their personal data?
- In the provided absence of the Data Subject's consent, has the Data Requestor provided a legitimate reason for you to share the patient/service user/staff member's personal or sensitive information with them.
- What permissible powers and legal exemptions are being relied upon to share or process personal data? These are described in Section 9: Legal gateways, exemptions and explicit powers.

5.2 It is good practice to have a partnership Data Sharing Agreement (DSA) in place at a local level to support this process. It is important that this agreement is signed by the appropriate senior level member of staff, (usually the Senior Information Risk Owner) for each NHS organisation.

5.3 **Providing a 'form of words':**

5.3.1 In cases where informed consent has not been sought from the Data Subject, has the Data Requestor explained in broad terms why they require to share and process the Data Subject's personal data? In other words, has the Requestor defined the legal justification clearly i.e. that there are **tangible public interest/best interest considerations where the individual is at risk of being drawn into terrorism and by informing the Data Subject, we may prejudice the intended outcome or lead to further harm.**

5.3.2 This baseline information will then enable the health provider to satisfy themselves that:

- There are tangible public interest/best interest considerations for providing the data/information being requested;
- The relevant public interest/best interest exemptions will therefore override your duty to protect the confidentiality of patient information;
- It is legitimate to provide information specific to the safeguarding concern which has been identified by the Data Requestor.

5.4 **Being specific:**

5.4.1 Data Requesters should clearly explain to you in writing what specific/relevant information is required from the patient/service user/staff member record to assist with the Prevent case management of the individual in question. It is important to note that if the request is not specific and relevant, the data should not be shared until further clarity has been sought, and the agreed timescales may not be met without this important information.

5.4.2 Health providers should only release personal data, which is relevant, necessary and proportionate to the public interest described in the request. This will always come down to your own professional judgement and be based on the nature of the inquiry and the information provided by the Data Requestor.

6. Case-by-Case Decisions

6.1 Each instance where personal or special category data is to be shared for Prevent purposes should be decided through a case-by-case assessment by the health professional.

This should consider:

- whether the informed consent of the individual can be obtained;
- any legal exemptions which are being relied upon as described in Section 9: Legal Gateways, Exemptions, and Explicit Powers, and
- that the proposed data/information sharing, and processing is necessary, proportionate and lawful.

6.2 If it has been decided that seeking consent from the individual to refer them to Prevent or share their personal data with a third party is not appropriate, you should always clearly document your decision and rationale in the patient record i.e. explain which public interest/best interest considerations have been applied to set aside their rights under the CLDC, the DPA 2018/ HRA 1998.

6.3 Additionally, health practitioners may often be required to share limited and proportionate data prior to seeking informed consent when this is urgently required to establish whether a case should be managed under Prevent or escalated as a counter terrorism case. This must also be on a case-by-case basis carried out in line with the public interest principles.

6.4 Any disclosures or discussions on data sharing or consent must always be documented in the patient record.

7. Channel and Other Partners

7.1 Prevent relies on early and effective information sharing to protect vulnerable individuals from being drawn into radicalisation, and part of this process is being able to build up an accurate picture of the level and extent of a person's vulnerability and identify any relevant protective factors. This data will to help inform any help or support which may be required for the individual, including through the Channel process.

7.2 **Section 38 of the Counter-Terrorism and Security Act 2015** (amended by the **Counter-Terrorism and Border Security Act 2019**), requires Channel partners to co-operate with the local authority and the police in providing any relevant information to the panel, so that they can effectively carry out their functions to determine whether an individual is vulnerable to being drawn into terrorism. Information should be provided in a timely manner subject to the requirements as detailed in Section 5: Responding to Data requests from Other Partners being fully met by the Requestor.

7.3 It is also important to note that the support received through Channel remains voluntary and section 36(4)(b) of the CTSA 2015 requires consent to be given by the individual to participate in any interventions. All individuals who receive support through Channel must be made aware of and consent to this as part of a programme. They must fully understand what the aims of the programme are and what to expect, including that their personal data may be shared with specific third parties as part of their support plan.

7.4 **Vulnerability Support Service**

7.4.1 Vulnerability Support Service (VSS) are multi-disciplinary mental health teams that work collaboratively with the police and health providers to safeguard individuals who have mental health vulnerabilities and who are at risk from radicalisation. Mental health practitioners from the VSS may liaise with health care providers either to provide information to support safeguarding or to clarify whether a safeguarding issue exists. Staff from the VSS will always state what their role is and what the suspected safeguarding issue is when requesting information.

8. Key General Principles of Data Sharing

8.1 The **DPA 2018** and **GDPR** act as a framework on how to process and share Personal Data with trusted partners. In common with all safeguarding matters, information sharing for Prevent purposes must comply with the relevant legislation, i.e. **DPA 2018**, **HRA 1998** and the **CDLC** (amongst others), and meet the same standard required for sharing information in respect of any other safeguarding concern.

8.2 **Lawfulness of information sharing and data processing:**

8.2.1 DPA 2018

The DPA 2018 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 either on its own or with other information',* i.e. sensitive personal data (including information about an individual's health, criminal record, and political or religious views). The Act also states the circumstances and extent to which this type of data can be processed.

The GDPR which underpins Chapter 2, Part 3 of the DPA 2018 is based around **six key data protection principles** and provides a range of rights for individuals which are applicable to the processing or sharing of personal and sensitive data. The principles state that personal data must:

- be processed lawfully, fairly and in a transparent manner;
- be processed for specified, explicit and legitimate purposes and not in any manner incompatible with those purposes;
- be adequate, relevant and limited to what is necessary in relation to the purposes;
- be accurate and up to date;
- not be kept for longer than is necessary, and
- be held securely.

8.3 **Personal data**

8.3.1 Personal data is any information which is related to an identified or identifiable natural person e.g. name address, telephone number, customer number or an online identifier.

Special category data is a sub-category of personal data that needs more protection because it is of a particularly sensitive nature, e.g.:

- Personal data revealing racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data and biometric data processed for the purpose of uniquely identifying a natural person;
- Data concerning health, or
- Data concerning a natural person's sex life or sexual orientation.

8.4 **Article 6** of the GDPR requires that organisations have a valid lawful basis for processing personal data. There are six lawful bases for processing; consent, contract, legal obligation, vital interests, public task and legitimate interests.

8.5 **Article 9** of the GDPR prohibits the processing of special category data. There are 10 exceptions to this prohibition which are referred to as conditions for processing special category data:

a) Explicit consent
b) Employment, social security and social protection
c) Vital interests

d) Not for profit bodies
e) Made public by the Data Subject
f) Legal claims of judicial acts
g) Reasons for substantial public interest (with a basis in law)
h) Health or social care (with a basis in law)
i) Public health (with a basis in law)
j) Archiving research and statistics (with a basis in law)

8.6 **Lawful, Transparent, Fair**

The six data protection principles listed in **Chapter 2 of Part 3 to the DPA 2018** must be complied with when sharing personal data, but the first data protection principle is particularly relevant. It states that the processing of personal data for any of the law enforcement purposes must be lawful and fair. 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.

8.7 To disclose data into the Prevent programme the lawfulness of the processing of the personal data must meet one of the conditions found in **Article 6** of the GDPR.

8.8 If any special category data is to be disclosed, then one of the conditions of **Article 9** of the GDPR must also be met (such as '**exception g**' 'Reasons for substantial public interest (with a basis in law)')**.**

8.9 The primary conditions for disclosing and processing personal data for the purposes of Prevent should always be on the basis of informed consent. However, as with any safeguarding concern, this may not always be appropriate or achievable. If consent is not appropriate or achievable, then a different lawful basis must be met in order to share personal data (see Section 9: Legal Gateways, Exemptions and Explicit Powers). If another lawful basis is not met, then personal data cannot be shared.

The exemptions contained in the DPA 2018 will specifically mean that an organisation can relieve some of its obligations contained under the legalisation. This includes:

- the right to be informed;
- the subject's right of access to personal data;
- dealing with other individual rights;
- reporting personal data breaches; and
- complying with the (data protection) principles.

Hence the sharing/disclosure of data can take place without the knowledge or consent of the individual.

8.10 **Data processing**

Part 3 of the DPA 2018[7] allows for the processing of personal data by a competent authority for the purposes of the detection and/or prevention of crime.

This provides a legitimate basis upon which a competent authority is permitted to share information for the prevention of crime and disorder, because it will be exercising a statutory function for law enforcement purposes. **Part 3 (Schedule 8)**[8] allows for the processing of sensitive data to safeguard vulnerable children or adults at risk from harm. A competent authority means:

- a person specified in **Schedule 7 of the DPA 2018**[9]; or
- any other person if, and to the extent that, they have statutory functions to exercise public authority or public powers for the law enforcement purposes.

Furthermore, if the sharing is to any organisation other than the Police, and if the disclosure is for the purposes of the prevention and detection of crime, then that receiving organisation must be a competent authority as defined by the DPA 2018, otherwise the disclosure cannot be made for this purpose.

9. Legal Gateways, Exemptions and Explicit Powers

9.1 In the vast majority of cases, information to be shared for Prevent purposes will contain special category personal data and so will need to satisfy one of the conditions in **Schedule 8** of the **DPA 2018**:

- The processing is necessary for the exercise of a function conferred on a person by an enactment or rule of laws and is necessary for reasons of substantial public interest (Schedule 8, condition 1: DPA 2018).
- The processing is necessary to protect the vital interests of the Data Subject or of another individual (Schedule 8, condition 3: DPA 2018).
- The processing is necessary for the purposes of protecting an individual from neglect or physical, mental or emotional harm, or, protecting the physical, mental or emotional well-being of an individual (Schedule 8, condition 4: DPA 2018).

9.2 There are also lawful exemptions set out in the DPA 2018 for requesting organisations to receive disclosed data for Prevent or for wider safeguarding purposes, where the consent of the individual or patient is inappropriate or unachievable.

Examples of exemptions which meet the Schedule 8 Conditions are contained in Schedule 2, Part 1 of the DPA 2018:

- Paragraph 10 of Part 2, Schedule 1 DPA 2018 (*Preventing or detecting unlawful acts*). This condition is met if the processing:

[7] https://www.legislation.gov.uk/ukpga/2018/12/part/3/chapter/3/enacted

[8] https://www.legislation.gov.uk/ukpga/2018/12/schedule/8/enacted?view=plain

[9] https://www.legislation.gov.uk/ukpga/2018/12/schedule/7/enacted

(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.

- Paragraph 18 of Part 2, Schedule 1 of the DPA 2018 (*Safeguarding of children and of individuals at risk*). This condition is met if the processing is necessary for the purposes of:

(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 aged
(i) under 18, or
(ii) aged 18 or over and at risk,

Part 2, Schedule 1 exemptions do not automatically supersede the Data Subject's right to be informed of the disclosure, this should always 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.

9.3 Section 115 of the Crime and Disorder Act 1998

The sharing of personal/special category data by public sector bodies requires the existence of a power to do so, in addition to satisfying the requirements of the DPA 2018, the HRA 1998 and the CLDC. Section 115 Crime and Disorder Act 1998 provides agencies and professionals with a permissive power (but not a legal duty) to disclose personal information for crime prevention purposes.

It provides that any person can lawfully disclose information, where necessary or expedient for any provision of the Act, to a Chief Officer of Police, a Police Authority, Local Authorities, Probation Provider or Health Authority (or to a person acting on behalf of any of these bodies), even if they do not otherwise have a power.

9.4 Common Law Powers to Share

Because the range of partners that the police work with 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 to do so. The decision to share using Common Law powers 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.

10. Other Relevant Legislation/Principles

10.1 HRA 1998:

Article 8 protects the right to respect for an individual private life, family life, home and correspondence (letters, telephone calls and emails, for example). There shall be no interference by a public authority 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 wellbeing 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.

10.2 **Article 8 of the European Convention on Human Rights (ECHR):**

Article 8 has particular relevance to Prevent. ECHR states that individuals have a right to respect for private and family life. The HRA further states that:

"*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*".

10.3 **CLDC:**

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. The 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 (see Section 9: Legal Gateways, Exemptions and Explicit Powers).

10.4 **The Caldicott Principles**

Principle 7 of the Caldicott Principles explains that duty to share information can be as important as the duty to protect patient confidentiality. Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Please remember that if in doubt, you should always consult with your Caldicott Guardian and or Data Protection Officer for your organisation for further advice and guidance before sharing personal or sensitive information for Prevent purposes.

11. Summary

11.1 Every health practitioner has a duty and must take responsibility for sharing the personal information and data that they hold regarding Prevent safeguarding concerns and should not assume that someone else will pass on this information, which may be critical in keeping someone at risk safe.

11.2 Confidentiality is an important ethical and legal duty, but it is not an absolute. You may disclose personal data without breaching duties of confidentiality in certain circumstances, particularly for safeguarding or public interest reasons. There are legal exemptions contained in the DPA 2018 and GDPR which allow for information sharing to take place in this context.

11.3 Each decision must be made on a case-by-case basis using your professional judgement and the rationale should always be recorded.

11.4 Fears about sharing personal data should not, therefore, be allowed to stand in the way of the need to safeguard and promote the welfare of children and adults at risk of abuse or exploitation.

11.5 Our partner agencies involved in information sharing are also subject to the same legal frameworks contained in the DPA 2018/GDPR and the same rigor must be applied when responding to external third-party information sharing with or from these bodies.

11.6 If in any doubt, you should always consult with your organisational Information Governance Team/Data Protection Officer, organisational Legal Advisor or Caldicott Guardian for further advice and guidance.

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:

- General Data Protection Regulations
- Data Protection Act 2018
- Common Law Duty of Confidentiality
- Information Commissioner's Office Guidance on Interpretation of the DPA 2018
- General Data Protection Regulations/ Data Protection Act 2018
- Caldicott principles as defined in 'The Information Governance Review'
- Crime and Disorder Act 1998
- European Convention on Human Rights
- Human Rights Act 1998
- Information sharing advice for safeguarding practitioners (HM Govt: 2018)
- DH – Code of practice on protecting the confidentiality of service user information (see page 43, chapter 5)
- GMC 'Confidentiality: good practice in handling patient information guidance' (May 2018)
- Royal College of Psychiatrists Good Psychiatric Practice: Confidentiality and Information Sharing (2nd edition) (CR209 Nov 2017)
- Prevent Duty Guidance 2015
- Channel Duty Guidance 2020
- HMG Mental Capacity Act 2005: Code of Practice
- Safeguarding children and young people: roles and competencies for health care staff intercollegiate Document: January 2019
- Working Together to Safeguard Children 2018
- Government Security Classification Policy 2018