North East Lincolnshire

Channel Information Sharing Agreement

Version 6.0

|  |  |
| --- | --- |
| Document owner  | Humber Prevent |
| Agreement number | HP001/19 |
| Document author and enquiry point  | Stewart Watson – NE Lincs, Channel Chair |
| Date of document  | August 2022 |
| Version  | 6.0 |
| Document classification  | Public  |
| Next document review date  | August 2024 |

**Contents**

[1. List of Partners to the Agreement 4](#_Toc110512971)

[2. Purpose of information sharing 4](#_Toc110512972)

[3. Information to be shared 5](#_Toc110512973)

[4. Basis for information sharing – legislative context 5](#_Toc110512974)

[5. Exchange of information 8](#_Toc110512975)

[6. Terms of use of the information 8](#_Toc110512976)

[7. Information and Data Quality Information 9](#_Toc110512977)

[8. Data retention review and disposal 10](#_Toc110512978)

[9. Access and Security 10](#_Toc110512979)

[10. General Operational Guidance/process 11](#_Toc110512980)

[11. Rights of the data subject 12](#_Toc110512982)

[12. Liability and Indemnity 12](#_Toc110512983)

[13. Management of the Agreement 12](#_Toc110512984)

[14. Closure/Termination of agreement 13](#_Toc110512985)

[15. Version History 13](#_Toc110512986)

[16. Agreement 13](#_Toc110512987)

Introduction

This Information Sharing Agreement has been developed to provide guidance for partners of the North East Lincolnshire Prevent Group. It is intended to operate within existing information sharing principles.

This Information Sharing Agreement (ISA) is an agreement between all agencies working together under the remit of Prevent and the Channel Process to share relevant information with agencies, in line with the Data Protection Act 2018 (DPA 2018) Section 8 and Schedule 2 Part 1(2) and the duty to co-operate under Section 38 of the Counter Terrorism and Security Act 2015 (CTSA 2015).

Section 38 of the CTSA requires partners (listed in Schedule 7 of the Act) to co-operate with the police in providing any relevant information. This is so that the police can make a fully informed risk assessment regarding the nature and extent of the person’s vulnerability and share the information with the local multi agency Channel Panel if appropriate. Partners should respond to the police **within 5 days** of any request where possible.

This agreement sets out the legal provisions relating to personal data sharing and takes account of the relevant Codes of Practice in respect of the sharing of personal data held by the Humberside Police, (the Management of Police Information Guidance and the ACPO Data Protection Manual of Guidance); and the Home Office Channel Guidance.

This agreement contains details of the standards agreed by the parties involved in the sharing of personal data and personally identifiable information so as to maintain confidentiality, integrity and compliance with the data protection principles, whilst ensuring that information is shared with those who ‘need to know’.

Requests for information from any of the parties to the agreement should be considered on a case-by-case basis in light of this agreement and the relevant legal parameters identified concerning the sharing of such personal data.

Information should not be disclosed to any persons who are not parties to this agreement, or if there is any doubt that the elements of this agreement are not in place, might be breached or not adhered to.

Any information will be dealt with securely and only shared with the local multi agency Channel Panel in accordance with the law and local information sharing agreements.

This agreement aims to facilitate the lawful and secure sharing of information between partner agencies and designated workers working to safeguard adults, children and young people.

### List of Partners to the Agreement

The North East Lincolnshire Channel Panel which consists of the following organisations:

* Humberside Police
* North East Lincolnshire Council
* North East Lincolnshire Clinical Commissioning Group
* National Probation Service
* East Midlands Ambulance Service
* Humberside Fire and Rescue
* Lincolnshire Partnership NHS Foundation Trust
* NAViGO
* Focus CIC
* Home Office
* Northern Lincolnshire and Goole NHS Trust

The partners to this agreement are also bound by the conditions set out in the Humber Information Sharing Charter.

### Purpose of information sharing

The purpose of this agreement is to enable the disclosure of information between the parties in accordance with the aims of the CHANNEL Project and data protection legislation.

The CHANNEL Project supports the Home Office Prevent Strategy, in ‘preventing terrorism by helping individuals to resist processes designed to turn them to violently extreme behaviour.’

Specifically, it aims to identify individuals and networks that are turning to violent extremisms or who are vulnerable to becoming so and those individuals and networks that seek to turn others to such behaviour, to enable measures to be developed aimed at facilitating the delivery of effective interventions and so divert vulnerable persons from turning to violently extreme behaviour.

The direct purpose of the CHANNEL Project is in accordance with the policing purpose as defined in the Code of Practice for the Management of Police Information:

* Protecting life and property
* Preserving order
* Preventing the commissioning of offences
* Bringing offenders to justice
* Any duty or responsibility of the police arising from common or statute

Only relevant, accurate and proportionate information will be disclosed to help partners to carry out safeguarding duties for which the data is required.

### Information to be shared

The agreement concerns the following personal and/or special categories of personal data (sensitive data) which needs to be shared for the purposes outlined in section 2.

* “Personal data” which identifies the person(s) at risk or alleged perpetrator(s) e.g. name, date of birth, address
* “Special categories of personal data / Sensitive data” about the alleged person(s) at risk victim(s) or alleged perpetrator(s) e.g. gender, religion, ethnicity
* Reasons for concerns and details of the alleged concerns e.g. type of radicalisation/extremist views, location, levels of risk or urgency
* Information about the physical and or mental health of the alleged person(s) at risk or alleged perpetrator(s) e.g. mental capacity, communication needs
* Reports of any medical or social care assessments or examinations undertaken as part of safeguarding procedures e.g. eligibility for community care, psychiatric assessment
* Personal data which identifies professionals involved with the alleged person(s) at risk or alleged perpetrator(s)
* Personal data which identifies other people who may be at risk e.g. via employment, family, service
* Historical information held in records about the alleged person(s) at risk or alleged perpetrator(s) that may be relevant to the current concern or case review e.g. previous safeguarding alert
* Name and contact details of alerter (unless they have stated they wish to remain anonymous and this anonymity would not have a detrimental impact upon the process)
* Name of employer or organisation
* The agreement also concerns aggregated data (e.g. statistics) which may be shared. In these situations, anonymised information **must** be used

### Basis for information sharing – legislative context

Partners to this agreement will act within existing legislative standards when protecting person’s vulnerable to violently extreme ideology.

The processing of information will satisfy:

* Article (6) (1) General Data Protection Regulation 2016 (UK GDPR)
* Article 9 (2) UK GDPR
* Section 38 of the Counter Terrorism and Security Act 2015
* Section 115 of the Crime and Disorder Act 1998
* Data Protection Act 2018 - Section 8 and Schedule 2 Part 1 (2) - Crime & taxation: general. This applies where personal data is disclosed by an organisation to the police for the purposes of the prevention or detection of crime or the apprehension or prosecution of offenders.
* The Data Protection Act 2018 - Section 28- National Security - Personal data is exempt if the exemption from that provision is required for the purpose of safeguarding national security (p3)
* Section 8(1) of the Human Rights Act 1998 - Right to a private life – All data subjects have a right to a private family which can only be interfered with if justified and proportionate. Interference with this right is justified because the processing is necessary and in the interest of:

Discharging the common law police duties

Preventing/detecting unlawful acts

Protecting public against dishonesty, etc.

Preventing fraud

Preventing Terrorist finance / money laundering

Safeguarding children and adults at risk

Safeguarding economic wellbeing of vulnerable adult

* Common law duty of care
* Common law duty of Confidence
* Consent given by the Adult

*General Data Protection Regulation*

Partners must meet the requirements of Article 6 of the UK GDPR, for the processing of personal data by virtue of subsections 1 (c), (d) and (e):

(c) processing is necessary for compliance with a legal obligation to which the controller is subject)

(d) the processing is necessary in order to protect the vital interests of the data subject or of another natural person

(e) 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;

In the case of sensitive personal data, partners must also meet Article 9 condition by virtue of subsections 2(b), (c) and (g):

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) 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;

(g) 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;

*Section 38 CTSA 2015 (Co-operation)*

(1)The partners of a panel must, so far as appropriate and reasonably practicable, act in co-operation with—

(a) the panel in the carrying out of its functions;

(b) the police in the carrying out of their functions in connection with section 36.

(2)The partners of a panel are the persons and bodies specified in Schedule 7.

(3)The duty of a partner of a panel to act in co-operation with the panel—

(a) includes the giving of information (subject to subsection (4));

(b) extends only so far as the co-operation is compatible with the exercise of the partner's functions under any other enactment or rule of law.

(4)Nothing in this section requires or authorises the making of—

(a) a disclosure that would contravene the data protection legislation;

(b) a disclosure of any sensitive information.

### Exchange of information

Information will be exchanged when a partner organisation believes that an individual is vulnerable to radicalisation or violent extremism or being exposed to those individuals and networks that seek to turn others to such behaviour.

Information discussed by the agency representative within the ambit of Channel is strictly confidential and must be treated as such during the meeting and in the subsequent handling of any data considered at this meeting, and must not be disclosed to third parties without the prior agreement of the partners of the meeting.

Information shared should be directly or indirectly relevant to cases. Clear distinctions should be made between fact and opinion.

All agencies should ensure that the minutes of all meetings are retained in a confidential and appropriately restricted manner. These minutes will aim to reflect that all individuals who are discussed at these meetings should be treated fairly, with respect and without improper discrimination. All work undertaken at the meetings will be informed by a commitment to equal opportunities and effective practice issues in relation to race, gender, sexuality and disability.

The responsibility to take appropriate actions rests with individual agencies. The role of the Channel Panel is to facilitate, monitor and evaluate effective information sharing to enable appropriate actions to be taken to increase public safety.

### Terms of use of the information

The information that is shared will be used to assess the risk posed to an individual at risk of radicalisation or violent extremism or being exposed to those individuals and networks that seek to turn others to such behaviour.

Information will be shared on a need to know basis only.

Any sharing of personal information must comply with the fair processing conditions outlined in the UK GDPR and any supporting data protection legislation. Consequently data should be:

* only be processed for the purposes detailed in section 2 and not further processed in a manner incompatible with those purposes
* adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’)
* accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’)
* kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’)
* processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’)
* For retention and destruction please see section 8 below

The disclosure of the information must lead to a proportionate response when protecting a vulnerable person or persons.

Caldicott Principles will also apply to the processing of the information (see Appendix B):

* Where it is reasonably determined that further information is necessary to fulfil statutory duties and/or other requirements this Agreement will be reviewed in full or in part as appropriate
* Whenever possible data shared, should be anonymised, unless requested at personal level
* Information on children, young people and adults will be shared with industry standard security
* All parties will store “person identifiable” data shared between both partners on secure systems which can only be accessed by a restricted number of appropriate staff with appropriate security safeguards
* All parties will use the data supplied for the purposes stated and will not pass such data to third party organisations outside the remit of specified partners in agreement without prior written consent
* It is also prohibited under this agreement for sub-processors to be used without the prior consent of the Data Controller
* All parties will comply with their obligations under the Freedom of Information Act 2000 and may consult with the other party if necessary if requests relate to information shared but will remain responsible for responding to the request

### Information and Data Quality Information

Each partner must recognise the importance of decision making based on information derived from robust systems and processes. All processes will be designed to support good quality data.

Information shared must be fit for purpose, which means that it must be adequate, relevant and limited to what is necessary in relation to the purpose for which they are being processed.

Information discovered to be inaccurate, out-of-date or inadequate for the purposes detailed in section 2 should be notified to the Data Controller – the original partner who has provided the information – who will be responsible for correcting the data and notifying all other recipients of the information who must make sure the correction is made.

Each partner will keep appropriate records of the sources of information to provide for this.

No secondary use or other use may be made unless the consent of the disclosing partner to that secondary use is sought and granted or required by law.

### Data retention review and disposal

Each partner to this agreement will ensure that they have in place policies and procedures governing:

1. The secure storage and protection of all personal data within their manual and electronic storage systems
	1. Electronic copies of information should only be held on encrypted devices or servers and should not be transferred to portable devices unless such devices are fully encrypted and their use is necessary for the provision of services under this agreement
2. The retention of information held in both manual and electronic systems is in accordance with legal requirements or agreed standards
	1. Information is only retained for the minimum period necessary in relation to the purpose for which it is held
3. The secure disposal of electronic and manually held information at the end of its retention period in accordance with their own secure destruction policy
	1. Electronic information should be securely destroyed by the physical destruction of the storage media or by the use of electronic shredding software that meets government standards or ISO 27001 to ensure permanent deletion
4. Hard copy information should be destroyed by cross-cut shredding. The information will be reviewed every 5 years to confirm that it remains accurate and relevant by the Gold Prevent Chair

### Access and Security

Each Partner will make sure that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

In particular, each partner shall make sure that measures are in place to do everything reasonable to:

* make accidental compromise or damage unlikely during storage, handling, use, processing transmission or transport
* deter deliberate compromise or opportunist attack
* securely dispose of or destroy the data in a manner to make reconstruction unlikely
* promote confidentiality in order to avoid unauthorised access
* be ready and prepared to respond to any breach of security swiftly and effectively and the partner must ensure that any breaches are reported to the Data Controller within one working day.
* maintain a record of personal data and processing activities regarding the data

Partners are expected to train their relevant staff and promote awareness of the major requirements of information sharing, including responsibilities in confidentiality and data protection.

Access to information subject to this agreement will only be given to those professionals who ‘need to know’ in order to effectively discharge their duties. Information will only be communicated through the agreed channels.

### General Operational Guidance/process

All partners to this agreement acknowledge and agree that the Information held will be processed fairly and lawfully in accordance with the principles of the DPA 2018 / UK GDPR or any relevant data protection legislation that applies.

All complaints or breaches relative to this agreement will be notified to Humberside Gold Prevent Chair and the designated Data Protection Manager of the relevant partner organisation as soon as possible and within one working day in accordance with their own policy and procedures.

Disclosure of personal information without consent must be justifiable on statutory grounds, or meet the criterion for claiming an exemption under the UK GDPR. Without such justification, both the partner and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the UK GDPR or damages for a breach of the Human Rights Act 1998.

If the disclosure of information is in contravention of the requirements of the UK GDPR, the partner who originally breached the requirements of the UK GDPR, either in requesting or disclosing information, shall indemnify the other partner against liability, cost or expense reasonably incurred.

### Rights of the data subject

In the processing of person data for the purpose of this agreement, data subjects will be notified and able to exercise their rights as set out in the UK GDPR / DPA 2018, subject to any exemptions that may apply.

### Liability and Indemnity

Under UK GDPR, Data Subjects are able to take action against both [Data] Controllers and [Data] Processors and potentially claim damages where they have suffered material or non-material damage as a result of an infringement of obligations under the UK GDPR (“Compensation”). The Information Commissioner’s Office can also fine a Processor or a Controller in relation to any breaches of data protection legislation.

Each partner to this Agreement will undertake to indemnify the others against any legal action arising from any breach of this Agreement by any person working for or on behalf of its own organisation.

In the event that the Data Controller or the Data Processor (for the purposes of this clause: “Party A”) is ordered by a Court/Tribunal to pay Compensation to a Data Subject or is required to pay a fine by the Information Commissioner’s Office, to the extent that such Compensation has arisen as a result of the act, negligence, omission or default of the other party (“Party B”), Party B shall indemnify Party A in respect of that element of the Compensation.

### Management of the Agreement

The agreement will be reviewed 2 yearly and monitored by the Humberside Gold Prevent Chair, unless new or revised legislation or national guidance necessitates an earlier review.

Complaints will be dealt with in a sensitive manner and recorded to enable the review and monitoring processes to be ethical. All complaints relevant to the sharing under this agreement will be dealt with by the relevant Channel Chair or Prevent Gold Chair.

Requests for information under the Data Protection Act and Freedom of Information Act 2000 will be dealt with by the designated Data Protection Officer of the relevant partner in accordance with their own policy and procedures.

Where a request for information includes that information provided by a partner organisation, the originating organisation will be informed in accordance with normal protocols. However, each organisation is responsible for their compliance with the Freedom of Information Act 2000.

It is the responsibility of each partner to the agreement to ensure that they have the latest version of this agreement.

All partners to the Agreement acknowledge and agree to comply with this agreement.

### Closure/Termination of agreement

This Agreement may be suspended by any partner for up to 30 days, in the event of any significant breach in order to negotiate appropriate remedial action*.*

Where negotiations do not successfully resolve the concerns of any partner, the agreement may be terminated in writing with immediate effect.

### Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date issued**  | **Version**  | **Status**  | **Reason for change**  |
| **June 2020** | **0.2** | **Draft** | **New Policy** |
|  |  |  | **Review and comments**  |
| **February 2022** | **0.3** | **Review** | **Comments** |
| **March 2022** | **0.4** | **Draft** |  |
| **August 2022** | **0.5** | **Draft** | **Comments** |

### Agreement

Agreement for < Organisation Name>:

We accept that this Information Sharing Agreement will provide a framework between the signatory organisations for the secure sharing of information within the Humberside Prevent Agenda in a manner compliant with our statutory and workers responsibilities.

**SIGNED……………………………………………..**

 **DATED……………………………………………...**

**Appendix A**

**The UK General Data Protection Regulation**

**Principles**

1. Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

1. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

Specific Articles – 6 & 9

Article 6 conditions relevant for purposes of processing of any personal data

1) Processing shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e) 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;

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Article 9

conditions relevant for purposes of processing of special categories of data

(1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.

(2) Paragraph 1 shall not apply if one of the following applies:

 a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c) 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;

d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e) processing relates to personal data which are manifestly made public by the data subject;

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g) 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;

h) 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;

i) 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;

j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on 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.

**Appendix B**

**Caldicott Principles**

The Caldicott Report set out a number of general principles that health and social care organisations should use when reviewing its use of client information and these are set out below:

**Principle 1**: Justify the purpose(s)

Every proposed use or transfer of personally identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by the appropriate guardian.

**Principle 2**: Do not use personally identifiable information unless it is absolutely necessary. Personally identifiable information items should not be used unless there is no alternative.

**Principle 3**: Use the minimum personally identifiable information.

Where the use of personally identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiably.

**Principle 4**: Access to personally identifiable information should be on a strict need to know basis.

Only those individuals who need access to personally identifiable information should have access to it.

**Principle 5**: Everyone should be aware of their responsibilities.

Action should be taken to ensure that those handling personally identifiable information are aware of their responsibilities and obligations to respect patient/client confidentiality.

**Principle 6**: Understand and comply with the law. Every use of personally identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

**Principle 7:** The 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.

**Principle 8:** Inform patients and service users about how their confidential information is used. A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.