Overarching Information Sharing Protocol
Criminal Justice Liaison

Agreement between:

Hampshire & IoW Criminal Justice Liaison Group:

Signatories: Senior Information Risk Owner or as appropriate:
To be signed by each Organisation

Organisation		**Signature & Date**
Southern Health NHS Foundation Trust	**Katrina Percy** Chief Executive	
Hampshire County Council	**Andrew Smith** Chief Executive	
Hampshire Constabulary	**Alex Marshall** Chief Constable	
Surrey & Borders Partnership NHS Foundation Trust	**Fiona Edwards** Chief Executive	
Southampton City Council	**Alistair Neill** Chief Executive	
Southampton City PCT	**Bob Deans** Chief Executive	
NHS Solent Healthcare	**Ros Tolcher** Chief Officer	
NHS Hampshire	**Debbie Fleming** Chief Executive	
Isle of Wight NHS PCT	**Kevin Flynn** Chief Executive	
G4S Medical + Forensic Services (UK) Ltd	**Dr Tony Knight** Clinical Lead for Hampshire	
Hampshire & Isle of Wight Criminal Justice Board	**Simon Townley** Chair	
Wessex Youth Offending Team	**Ian Langley** Head of Service	
Solent Mind	**Richard Barritt** Chief Executive	
South Central Ambulance Service	**Will Hancock** Chief Executive	
Portsmouth City PCT	**Tracy Sanders** Chief Executive	

By signing this document all parties have agreed to accept and implement this protocol

1. INTRODUCTION

Many organisations are responsible for the provision of a wide range of services to the public which are often undertaken in cooperation with other organisations. One of the most vital resources in accomplishing this is the common availability of relevant information. Whilst there is a public expectation of appropriate sharing of information between organisations providing services to them, the public rightly expect that their personal data will be properly protected. When sharing personal information, organisations must ensure that the Principles of the Data Protection Act 1998, the Human Rights Act 1998, Caldicott Principles (for Health and Social Care), the Crime Disorder Act 1998 and the common law duty of confidentiality are upheld.

The effectiveness of information sharing relies on good relations and mutual trust but must also comply with legislative, regulatory and ethical demands and needs to be carried out in a consistent manner by all the parties involved. This Overarching Information Sharing Protocol ("the Protocol") provides the basis for facilitating the exchange of information between the organisations concerned where it is necessary or expedient under the terms of any legislation in order to provide services in the most effective and appropriate way. Appendix 1 provides details of the data protection contact or equivalent, for each member organisation of the Hampshire & Isle of Wight Mental Health & Criminal Justice Liaison Group.

(Please see Appendix 2 for an overview of the *Principles of the Data Protection Act 1998* and the 6 *Caldicott Principles and the NHS Confidentiality Code of Practice.*)

Legislative framework:

The Prevention of Terrorism Act 2005
Terrorism Act 2006
Anti-terrorism, Crime and Security Act 2001
The Road Traffic Act 1991
The Police and Criminal Evidence Act 1984
The Crime and Disorder Act 1998
The Data Protection Act 1998
The Freedom of Information Act 2000
Access to Health Records Act 1990
The Children Act 2004
Disability and the Equality Act 2010
The Mental Health Act 2007
The Mental Capacity Act 2005 including Deprivation of Liberty Safeguards (DOLS)
The Health & Social Care Act 2008 (Regulated Activities) Regulations 2010
The Human Rights Act 2000
The Criminal Justice and Immigration Act 2008
Se Offences Act 2003
Care Standards Act 2000
The Carers & Disabled Children's Act 2000
The Carer's Recognition and Services Act 1995
The NHS & Community Care Act 1990
Disabled Person's Act 1986
Race Relations Act 2000
Sexual Discrimination Act 1975
Chronically Sick and Disabled Persons Act 1970

2. DEFINTION

A protocol is an agreement between participants, in an information-sharing partnership to govern the sharing of information, satisfy the requirements of law and guidance, regulate working practices and provide operational guidelines in both the disclosing and receiving organisations.

Compliance with this Protocol is mandatory and could lead to disciplinary procedures if breached, for all employees of the organisations involved in the use of this Protocol.

This protocol is intended to ensure information is shared legitimately and appropriately between all the services mentioned in this ISP. Local operating guidance will be developed and implemented relating to specific circumstances – i.e. Missing persons.

3. OBJECTIVES

3.1 To provide an overarching framework for the maintenance and development of operational procedures to ensure appropriate sharing of information between party organisations.

3.2 To protect confidential personal information and ensure the effective sharing of information between signatory organisations and their services.

3.3 To draw on currently available guidance on the protection and use of confidential information and ensure that this is within the framework of professional codes of conduct and current legal requirements.

3.4 To comply with the recommendations from the Independent Police Complaints Commission Report "Police Custody as a "Place of Safety".

4. PRINCIPLES

In accordance with Department of Constitutional Affairs, Department of Health and Data Protection Act guidance on Information Sharing, Information Commissioners Code of Practice and Caldicott Principles, no information can be shared with anyone unless the subject consents – exceptions may be made in individual cases for any of the following reasons:

- Prevention and detection of crime
- Prevention and detection of crime and/or the apprehension or prosecution of offenders
- To protect vital interests of the data subject; serious harm or matter of life or death
- For the administration of justice (usually bringing perpetrators to justice)
- For the exercise of functions conferred on any person by or under any enactment (police/social services)
- In accordance with a court order
- Over-riding public interest
- Child protection – disclosure to social services or the police for the exercise of functions under the Children Act, where the public interest in safeguarding the child's welfare over-rides the need to keep the information confidential
- Right to life
- Right to be free from torture or inhuman or degrading treatment

5. CONSENT

Obtain Consent:

Wherever possible, practical, and safe to do so, the data subject's consent to release information should be obtained. However, there may be times when this is not possible due to the data subject's condition, for example the data subject is unconscious or has absconded, or has been discharged from the care of the providing service, or where gaining consent is likely to result in further incidents or risk.

Disclosure of information to the Police without the data subject's consent:

The consultant in charge of the data subject, or their deputy, has discretion, within the law, over what information may be given to the Police. This may either be by the provision of copy extracts or being allowed to view the records during attendance by a Police Officer at the Trust's premises. Where police attend outpatient clinics, there may not always be a designated consultant with responsibility; in these cases the senior clinician will need to make the decision.

Requests for information under the provisions of Section 29 (3) of the Data Protection Act 1998 (DPA)

Section 29 (3) DPA provides police with an exemption to the non-disclosure provisions of the Act where the information required is for the prevention and detection of crime and or, the apprehension and prosecution of an offender.

There is no legal requirement for an officer of a specific rank to authorise the completion of a section 29(3) notice, referred to as a DP2 (see Appendix 3).

The DP2 forms an audit trail to the organisation the police are requesting data from as to what information is being requested, why and who has requested the data. Any ranking police officer can use this exemption.

Working practices should be the same throughout the Hampshire Constabulary area, as section 4.18 of the Force Procedure 2106 – Data Protection, outlines how the force should be using the DP2 form as part of their everyday business. This procedure indicates that where an organisation seeks further clarification the DP2 can be countersigned by a supervising officer (no rank specified) to provide added confidence that the request is legitimate.

Officers found to have submitted a Section 29 (3) request that is not part of a legitimate police investigation, would be subject to disciplinary proceedings and possibly criminal proceedings through the courts for offences under Section 55 of the Data Protection Act.

Circumstances where information may be released:

If the public interest and safety out-weighs the duty of confidentiality; this is likely to involve crimes of a very serious nature or where a serious offence is being investigated, See list below:

- Murder or Attempted Murder
- Manslaughter
- Rape both Sect 1 (penetration of the vagina, anus or mouth using his penis) or Sect 2 offences (assault by penetration of the vagina or anus with a part of the body or a thing, or both)
- Kidnapping

- Sexual activity with a child family member, boy or girl under 13
- Sexual assault by touching boy or girl under 13 / under 16 without consent
- Causing an explosion likely to endanger life or property
- Possession of firearms with intent to injure
- Use of firearms and imitation firearms to resist arrest
- Carrying firearms with criminal intent
- Hostage taking
- Hijacking
- Offences under Sections 1,9 and 10 of the Prevention of Terrorism (Temporary Provisions) Act, 1984.

Prevention of Terrorism Act (1989) and Terrorism Act (2000) – information (including personal information) about terrorist activity MUST be disclosed to the police. It is a statutory duty to do so.

If the provisions of Section 172 of the Road Traffic Act 1988 apply (name and address). Staff have a statutory duty to inform the Police, when asked, of the name and address of any driver who is allegedly guilty of an offence under the Act; it is not necessary to disclose clinical information. Where the investigation concerns offences involving motor vehicles staff can provide the Police with service user/occupant/driver demographic details. Under Section 168 (2) (b) 0f the 1972 Road Traffic Act any person (e.g. Trust staff) must give information that may lead to the identification of the driver of a vehicle, where the driver is alleged to have committed an offence under the Act. It should be noted that the information is restricted only to enable an identification of the driver and no other information should be given. (Hunter-v-Mann 1974).

If the release is for the prevention and detection of crime and is a life or death matter and the decision has been made that its release is 'in the public interest and safety' then the appropriate information must be released and the organisations SIRO/Caldicott Guardian/Data Protection officer informed. The Police must provide a completed and signed DP2 form (see Appendix 3).

The Crime & Disorder Act (1998):

Information may be passed to the Police on an individual, if there is a need for strategic cross-organisation / multi-agency information sharing, to detect, prevent or reduce crime and disorder that an individual may be involved. There may also be requests for aggregated data (that does not directly identify individuals) for detection, prevention or crime reduction purposes. A public moral duty to furnish certain information about a data subject to the police over-rides the duty of confidentiality. i.e. there is sufficient public interest justification to release it.

There is provision in the Crime and Disorder Act 1988 that specifically allows police, local and health authorities to disclose information about individuals on the sex offender register who have also been identified as posing a significant risk to others.

The Police and Criminal Evidence Act (1984):

The Act creates a power to that allows information to be passed to the Police if there is a risk that someone may be seriously harmed or death may occur if the Police are not informed. Serious offences include, murder, rape, kidnapping (and all attempts to commit such offences) and causing death by dangerous driving.

Where it is evident to staff that they, colleagues or members of the public may be at risk and that involving the police or other agencies is appropriate. The Caldicott Guardian, or senior manager's agreement should always be obtained whenever possible. Examples include detained service users who are absent without leave or service users who are registered as missing persons.

6. CONFIDENTIALITY

Confidentiality is a key part of the clinician/service user relationship. As well as legislation governing the protection and use of personal data, a common law duty of confidentiality applies.

Personal data which is subject to the common law duty of confidentiality has a number of characteristics:

- The information is not in the public domain or readily available from another source
- The information is of a certain degree of sensitivity, e.g. medical data
- The information has been provided with the expectation that it will only be used or disclosed for particular purposes

Any breaches of confidentiality will be dealt with by each local organisation according to their policy – see section 8.

7. MANAGEMENT & REVIEW OF THE PROTOCOL

7.1. The holder of the master copy of this protocol will be the Caldicott Guardian of Southern Health NHS Foundation Trust

7.2. A copy of the protocol will be held by all organisations involved.

7.3. The protocol will be reviewed initially after one year and then subsequently every two years, and will be co-ordinated by the Criminal Justice Liaison Group.

7.4. Any agreed amendments will be completed and circulated by the holder of the master copy.

7.5. It will be each organisation's responsibility to ensure that any proposed amendments are shared at the Hampshire & Isle of Wight Mental Health Criminal Justice Liaison Group and an agreement reached on the method of handling the amendment. Agreed amendments to be made by the holder of the master copy and re-distributed to all organisations involved

7.6. Individual organisations are responsible for ensuring their staff receive clear guidance on their relevant policies and procedures including this Protocol

8. COMPLAINTS & BREACHES

8.1. All organisations should have their own internal procedures for dealing with breaches of confidentiality and complaints.

8.2. The employing organisation should instigate their internal procedures for breach of confidentiality.

8.3. The Caldicott Guardian/Senior Information Risk Owner/Data Protection Officer of the appropriate organisation should be notified immediately and all other parties should be informed.

8.4. The breach should be investigated and a final report with outcomes and actions should be presented to the Hampshire & Isle of Wight Mental Health Criminal Justice Liaison Group

8.5. Consideration should be given as to whether any information loss/breach is reported as a Serious Untoward Incident via the relevant risk reporting mechanism.

9. OPERATIONAL PROCEDURES

In order to provide practical guidance to staff from partner organisations, relating to the differing circumstances relating to the sharing of information, the following guidance is available.

10. Policies and reference information:

- *Information Sharing and Mental Health – Guidance to Support Information Sharing by Mental Health Services* – Dept of Health; August 2009

- *Police Custody as a "Place of Safety" – examining the use of Section 136 of the MHA 1983* – ipcc; September 2008

- *Multi-agency partnership working and the delivery of services to mentally disordered offenders* – nacro; 2005

Appendices:

Appendix 1: Data Protection contact within each member agency
Appendix 2: Principles of the Data Protection Act 1998; 6 Caldicott Principles; NHS Code of Confidentiality
Appendix 3: Sample Consent to Share Form
Appendix 4: DP2 – Hampshire Constabulary Request for Information Form
Appendix 5: Guidance for staff on information sharing
Appendix 6: Information Sharing Scenarios

Addendum List of Information Sharing Protocols agreed by each organisation (unique list for each organisation)

Appendix 1

Data Protection contact within each member agency of the Hampshire & Isle of Wight Mental Health Criminal Justice Liaison Group:

Organisation	SIRO / Data Protection Lead Name & Role
Southern Health NHS Foundation Trust 023 8087 4000	**Dr Huw Stone** Caldicott Guardian huw.stone@nhs.net
Hampshire County Council 01962 841841	**Liz McGill** Strategic Commissioning Manager (MH) liz.mcgill@hants.gov.uk
Hampshire Constabulary 01962 841534	**Simon Brown** Data Protection Officer simon.brown@hampshire.pnn.police.uk
Surrey & Borders Partnership NHS Foundation Trust 01883 383838	**Mandy Stevens** Director of Quality & Performance mandy.stevens@sabp.nhs.uk
Southampton City Council 023 8083 2798	**Linda Chan** Organisational Development Manager linda.chan@southampton.gov.uk
Southampton City PCT 023 8029 6064	**Gordon Cheeseman** Information Governence Manager gordon.cheeseman@scpct.nhs.uk
NHS Solent Healthcare 023 8060 8000	**Susannah Long** Business Assurance Manager susannah.long@solent.nhs.uk
NHS Hampshire 023 8062 7609	**Kathryn Long** Information Governence Manager kathryn.long@hampshire.nhs.uk
Isle of Wight NHS PCT 01983 524081	**Sandy Gilbert** Senior Commissioning Manager – Offender Health sandy.gilbert@iow.nhs.uk
G4S Medical + Forensic Services (UK) Ltd 01371 812600	**Dr Tony Knight** Clinical Lead for Hampshire tony.knight.g4s@forensicpages.com
Hampshire & Isle of Wight Criminal Justice Board 023 9244 0054	**Emma Robertson** Business Manager LCJB@hampshire.pnn.police.uk
Wessex Youth Offending Team 01962 876100	**Ian Langley** Head of Service ian.langley@hants.gov.uk
Solent Mind 023 8020 8940	**Richard Barritt** Chief Executive rbarritt@solentmind.org.uk
South Central Ambulance Service NHS Trust 01869 365000	**Barbara Sansom** Information Governence Manager barbara.sansom@scas.nhs.uk
Portsmouth City PCT 023 9282 2444	**Susannah Long** Business Assurance Manager susannah.long@solent.nhs.uk

8 Principles of the Data Protection Act 1998:

The eight principles of the new act apply to all staff handling personal date are, briefly that personal data (including service user – identifiable data) shall be:

1. Processed f**airly and lawfully** and not unless certain conditions are met.
2. Obtained only for **specified and lawful purposes**, and not further processed for any other.
3. **Adequate, relevant** and **not excessive** in relation to those purposes.
4. **Accurate** and where necessary, **kept up to date.**
5. **Kept for no longer than is necessary** for those purposes.
6. Processed in accordance with the **rights of the data subjects.**
7. Protected by **appropriate security measures** and:
8. **Not transferred** without an adequate level of protection.

6 Caldicott Principles (an NHS Directive):

There are considerable overlaps with the Data Protection Act and both combine to inform the conduct of staff in handling confidential information.

The six Caldicott principles applying to all staff handling service user-identifiable data, are:

1. Justify the purpose(s) of every proposed use or transfer;
2. Don't use it unless it is absolutely necessary, and
3. Use the minimum necessary;
4. Access to it should be on a strict need to know basis;
5. Everyone with access to it should be aware of their responsibilities
6. Understand and comply with the law.

NHS Code of Confidentiality:

This document outlines the legal requirements and reiterates the NHS ethos of providing a confidential service. It acknowledges that there are exceptional circumstances in which information may be released without consent, but is largely concerned with ensuring that NHS data handling procedures are within the legal framework.

Service users' identifiable information is held under a duty of confidentiality. This includes information about their condition, and where they are being treated. This means that such information should not normally be disclosed to anyone, unless the service user concerned has consented. In the absence of consent, confidentiality can only lawfully be breached if there is:

- a legal obligation to do so where the professional has no choice, e.g. a court order requiring disclosure; or
- an overriding public interest in disclosing the information where the professional must exercise judgement.

Unless the service user consents, this means that the person considering disclosure must be satisfied that there is an overriding public interest which justifies breaching the relevant service user's confidentiality.

When considering a disclosure of confidential information, a judgement will always be required about where the public interest lies; the more private and damaging the information, the stronger the public interest in disclosure will need to be. Disclosure of health information is particularly likely to cause harm and/or distress because of its very personal nature. Any disclosures must therefore be necessary and proportionate.

The Code of Practice advises that:
".. staff are permitted to disclose personal information in order to prevent and support detection, investigation and punishment of serious crime and/or to prevent abuse or serious harm to others where they judge, on a case by case basis, that the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual service user concerned and the broader public interest in the provision of a confidential service"

Appendix 3

SAMPLE FORM

CONFIDENTIAL

Information Sharing and Consent Form

RiO ID		NHS No.	
Client details			
Title	**Family Name**	**Given Name**	**Date of Birth**

Sometimes the Mental Health Trust's care team looking after you may include people from other organisations such as social services or education. Although this is routine, we will tell you if this is the case. As part of your care we may also have to contact external agencies who are not part of the NHS and who are not normally part of your care team. We will agree this with you beforehand, on each occasion that any of you information needs to be shared. If you don't agree, we will discuss with you the possible effect this may have on your care and the alternatives available. In any case, we will record what has been shared, and for what reasons, in the appropriate place in your record. In exceptional circumstances, there may be occasions where it is necessary to share information without your consent. This will be in accordance with Trust policy, common law and the Data Protection Act, as appropriate. For example, it may be disclosed where justified in the public interest to protect you or someone else from harm. In these circumstances the information shared will always be kept to the minimum necessary.

If there are any people, who are not healthcare professionals – such as relatives, or neighbors – who you DO NOT want us to contact, please give us their names / addresses and relationship to you.

Please record any comments the clients might have about sharing information

Has the client's signature been collected?	☐ Yes	☐ No

You, the client, can change the mind about any of the above at any time; let your care coordinator know

Complete by	Name + Signature:		
	Job title	Date:	Time:
	Team + Location:		

Client Signature		Date	

If no client signature obtained, please state the reason why:	

HAMPSHIRE CONSTABULARY

DP2

Declaration Form for Data User
RESTRICTED

PLEASE TREAT THIS ENQUIRY AS CONFIDENTIAL

RMS No | Operation Name

To

DATA PROTECTION ACT, 1998, SECTION 28 and SECTION 29(3)

I am making enquiries which are concerned with:

The prevention and detection of crime, or the apprehension or prosecution of offenders* ☐

National Security* ☐

The vital interests of the data subject* ☐

** One of these must be selected*

DATA PROTECTION ACT, 1998, PRINCIPLE 1, SCHEDULE 2/3

Information Required

Nature of enquiry

I confirm
the inforr

Signed

Name

Police Station

Countersigned
(where necessary)

Appendix 5

Seven Golden Rules for Information Sharing

1. **Remember that the Data Protection Act is not a barrier to sharing information** but provides a framework to ensure that personal information about living persons is shared appropriately.

2. **Be open and honest** with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. **Seek advice** if you are in any doubt, without disclosing the identity of the person where possible.

4. **Share with consent where appropriate** and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgment, that lack of consent can be overridden in the public interest. You will need to base your judgment on the facts of the case.

5. **Consider safety and well-being**: Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

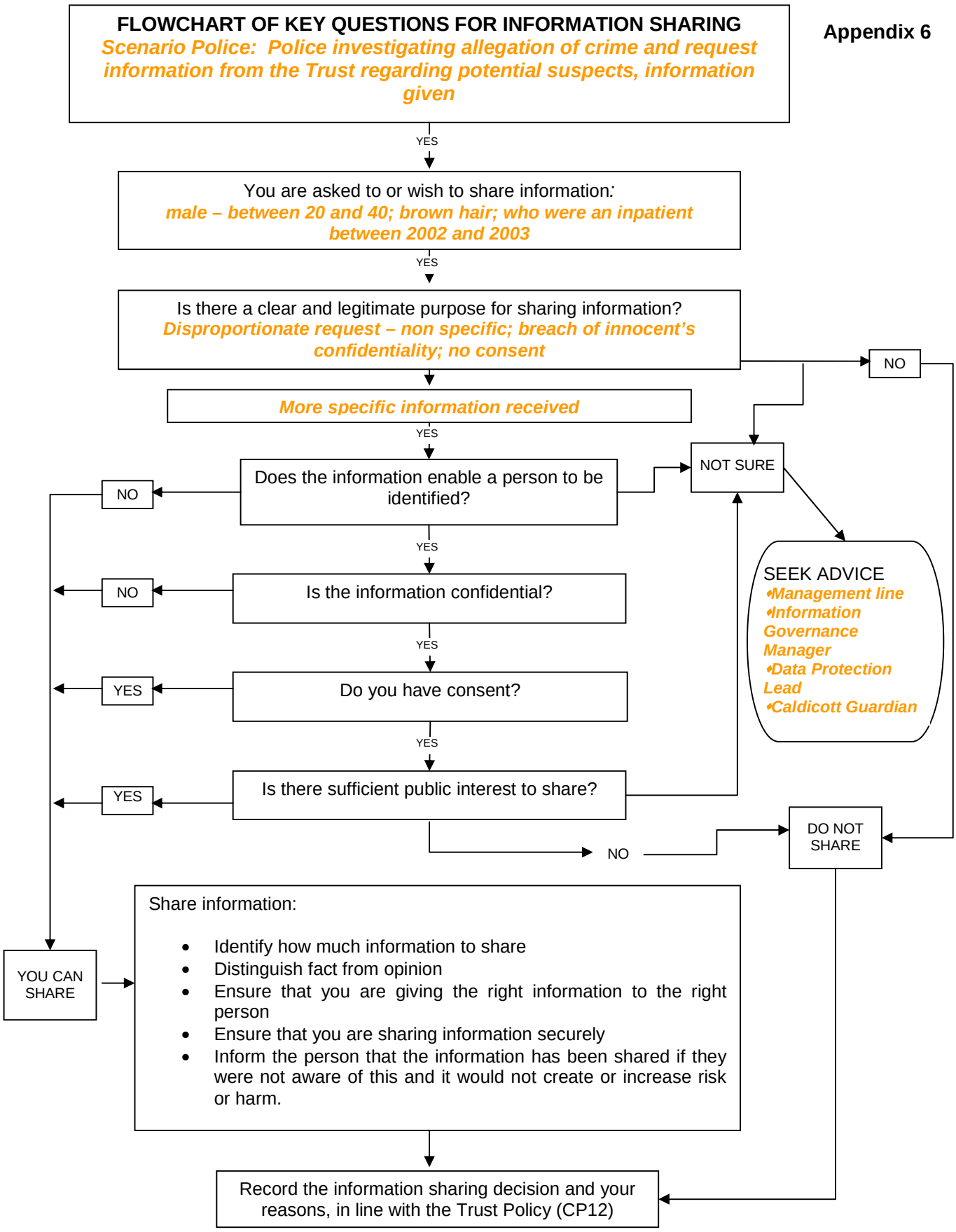
6. **Necessary, proportionate, relevant, accurate, timely and secure:** Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

7. **Keep a record** of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Appendix 6

FLOWCHART OF KEY QUESTIONS FOR INFORMATION SHARING

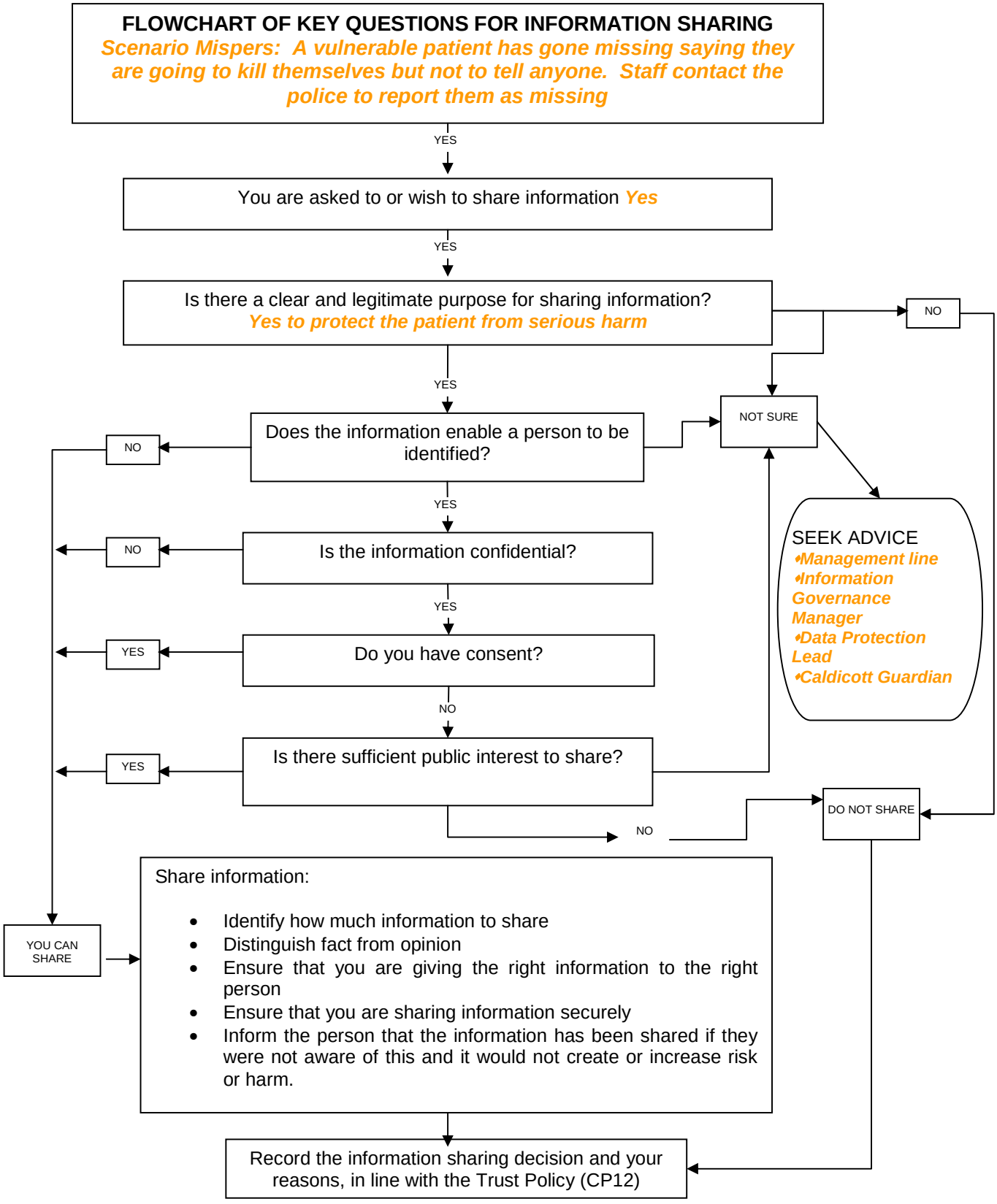
Scenario Police: Police investigating allegation of crime and request information from the Trust regarding potential suspects, information given



If there are concerns that a child may be at risk of significant harm or an adult may be at risk of serious harm, then follow the relevant procedures without delay.

Seek advice if you are not sure what to do at any stage and ensure that the outcome of the discussion is recorded.

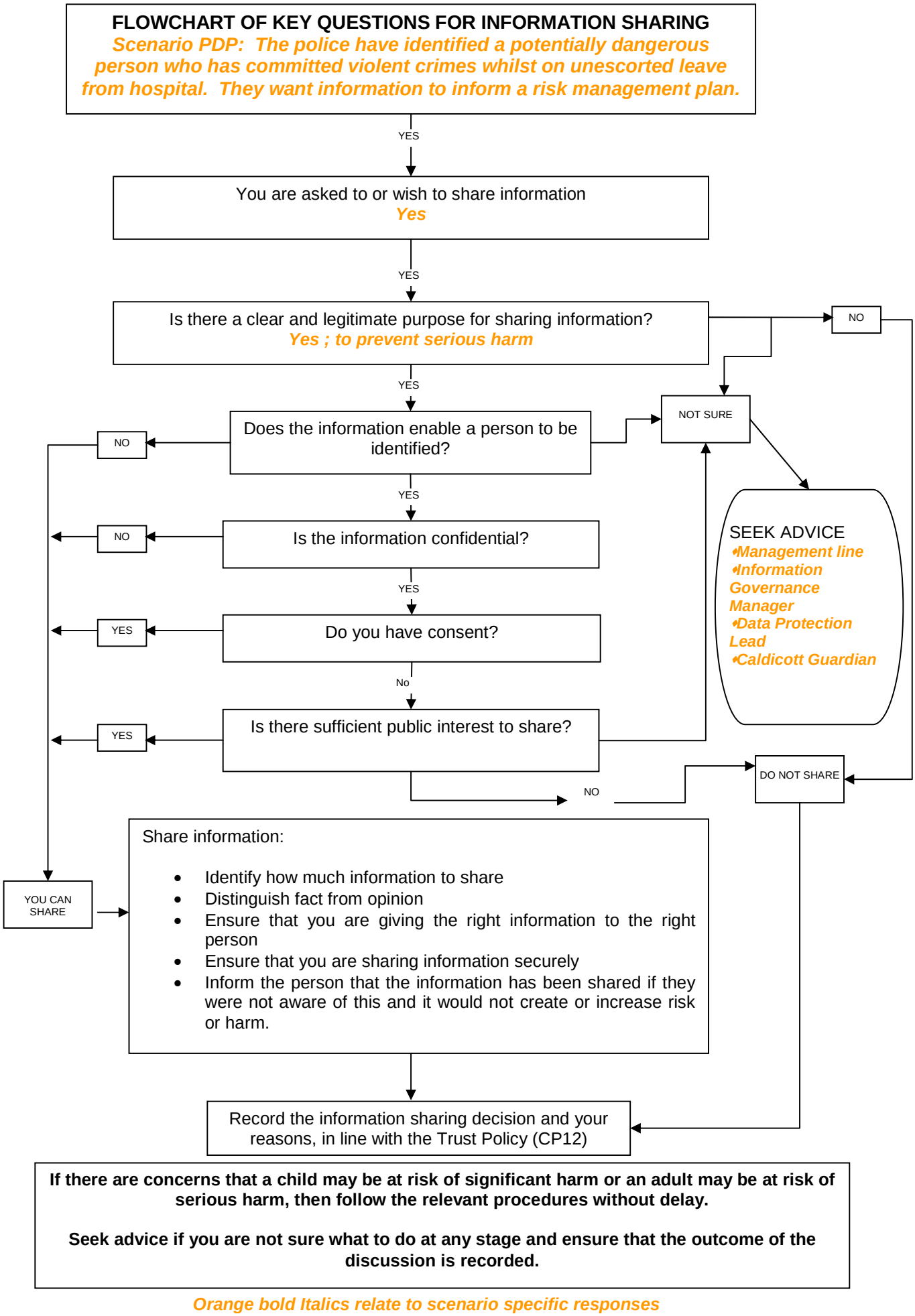
Orange bold Italics relate to scenario specific responses

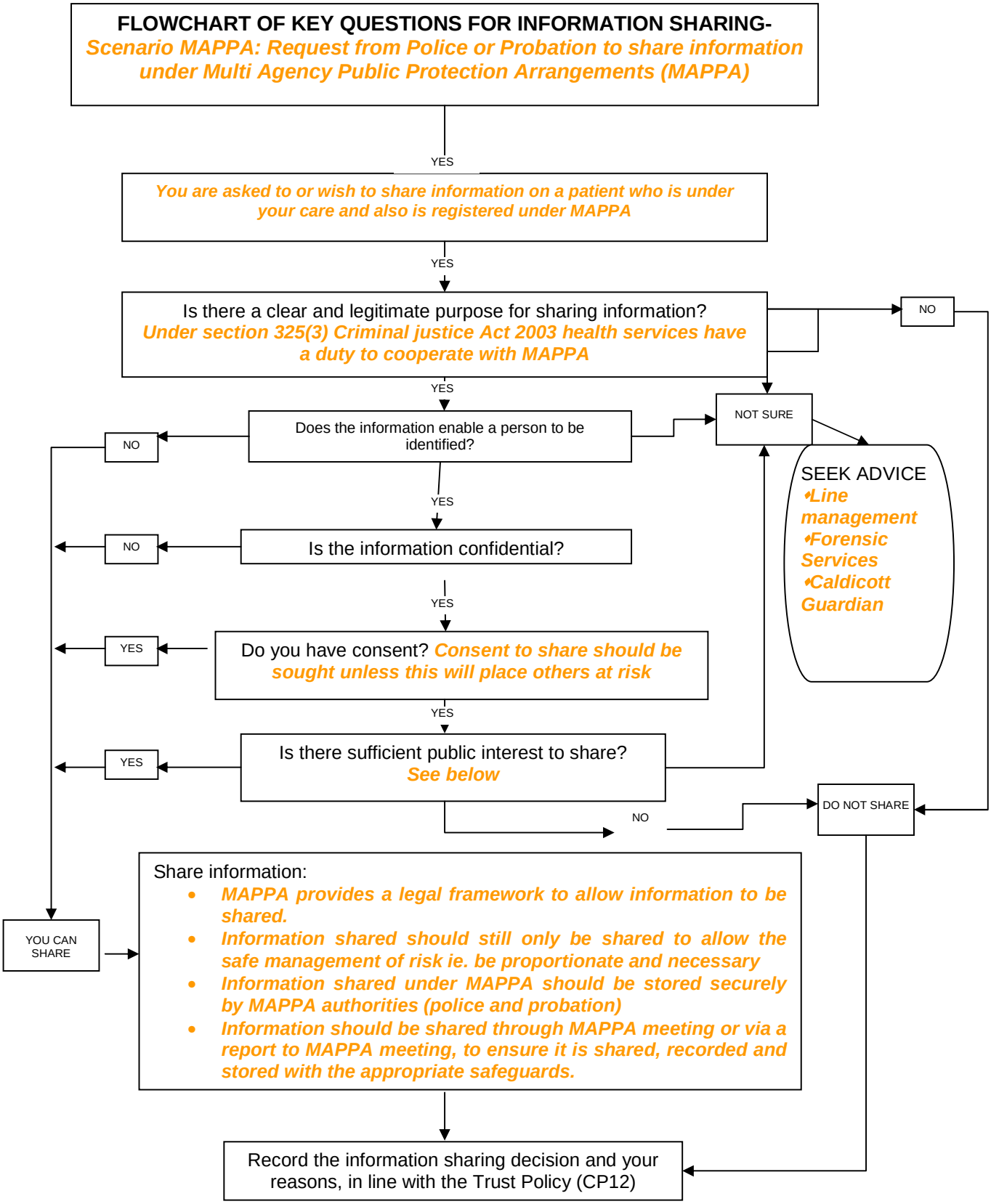


If there are concerns that a child may be at risk of significant harm or an adult may be at risk of serious harm, then follow the relevant procedures without delay.

Seek advice if you are not sure what to do at any stage and ensure that the outcome of the discussion is recorded.

Orange bold Italics relate to scenario specific responses


FLOWCHART OF KEY QUESTIONS FOR INFORMATION SHARING
Scenario PDP: The police have identified a potentially dangerous person who has committed violent crimes whilst on unescorted leave from hospital. They want information to inform a risk management plan.
YES
You are asked to or wish to share information
Yes
YES
Is there a clear and legitimate purpose for sharing information?
Yes ; to prevent serious harm
NO
YES
NOT SURE
Does the information enable a person to be identified?
NO
YES
SEEK ADVICE
•Management line
•Information Governance Manager
•Data Protection Lead
•Caldicott Guardian
NO
Is the information confidential?
YES
YES
Do you have consent?
No
YES
Is there sufficient public interest to share?
NO
DO NOT SHARE
YOU CAN SHARE
Share information:
Identify how much information to share
Distinguish fact from opinion
Ensure that you are giving the right information to the right person
Ensure that you are sharing information securely
Inform the person that the information has been shared if they were not aware of this and it would not create or increase risk or harm.
Record the information sharing decision and your reasons, in line with the Trust Policy (CP12)
If there are concerns that a child may be at risk of significant harm or an adult may be at risk of serious harm, then follow the relevant procedures without delay.
Seek advice if you are not sure what to do at any stage and ensure that the outcome of the discussion is recorded.
Orange bold Italics relate to scenario specific responses



Orange bold Italics relate to scenario specific responses

FLOWCHART OF KEY QUESTIONS FOR INFORMATION SHARING- ***Scenario MARAC: Request from Police - A woman with 2 children (14 and 9) has had three attendances at A &E over the last 2 months. The first was a fractured eye socket, second a burn to her arm and the third was a broken arm which she told A&E staff had been caused by her husband twisting it when he became angry with her. She says although he often gets angry with her he would never harm the children.***

The case is going to MARAC because she had recently revealed to a local domestic abuse organisation the fact that he had deliberately poured boiling water over her.

She does not want anyone to know what has happened as it may affect his job as a head teacher. She has been told about confidentiality and has specifically stated that she doesn't want the health authority to share her information.

Do you share relevant health info in the MARAC?

YES

Is there a clear and legitimate purpose for sharing information? - ***Yes. There are child protection concerns. It is unlikely that her perception of risk is balanced due to the circumstances she is in. The risk to her is serious (assessed as High to go to MARAC) and already she has been subjected to serious harm so it is likely that there is sufficient public interest to merit sharing information without her consent.***

NO

YES

NOT SURE

Does the information enable a person to be identified?

NO

YES

Is the information confidential?

NO

YES

Do you have consent? ***Consent to share should be sought unless this will place others at risk***

YES

Is there sufficient public interest to share? ***See below***

YES

NO

SEEK ADVICE

- ***Line Management***
- ***Forensic Services***
- ***Caldicott Guardian***

DO NOT SHARE

YOU CAN SHARE

Share information:

- Identify how much information to share
- Distinguish fact from opinion
- Ensure that you are giving the right information to the right person
- Ensure that you are sharing information securely
- Inform the person that the information has been shared if they were not aware of this and it would not create or increase risk or harm.

Record the information sharing decision and your reasons, in line with the Trust Policy (CP12)

If there are concerns that a child may be at risk of significant harm or an adult may be at risk of serious harm, then follow the relevant procedures without delay.

Seek advice if you are not sure what to do at any stage and ensure that the outcome of the discussion is recorded.

Orange bold Italics relate to scenario specific responses

FLOWCHART OF KEY QUESTIONS FOR INFORMATION SHARING

Scenario: 136 Place of Safety

26 year old woman detained by police – taken to PoS. Nurse requests information from Police re. circumstances, e.g. self harm; violence; alcohol/drug use. MHA assessment to be completed by AMHP & 2 doctors. Info requested from police re. past offending. Review of available info identifies potential child at risk (4 yr old). Patient will not consent to contact being made with key worker or Probation Officer. AMHP requests info from Child Services re. child; from Probation & Substance Misuse Service re. current involvement. Patient discloses to doctor that she received care from London Psychiatric Unit – but does not want doctor to contact unit.

Do you share relevant health info?

YES

Is there a clear and legitimate purpose for sharing information? - ***Yes. All agencies need to share relevant and pertinent information as there are child safety/protection issues, and to complete a full and accurate MHA assessment. It is unlikely that her perception of risk is balanced due to the circumstances she is in and sufficient public interest to merit sharing information without her consent.***

NO

YES

Does the information enable a person to be identified?

NO

NOT SURE

SEEK ADVICE
- ***Line Management***
- ***Forensic Services***
- ***Caldicott Guardian***

YES

Is the information confidential?

NO

YES

Do you have consent? ***Consent to share should be sought unless this will place others at risk***

YES

YES

Is there sufficient public interest to share? ***See below***

NO

DO NOT SHARE

YOU CAN SHARE

Share information:
- Identify how much information to share
- Distinguish fact from opinion
- Ensure that you are giving the right information to the right person
- Ensure that you are sharing information securely
- Inform the person that the information has been shared if they were not aware of this and it would not create or increase risk or harm.

Record the information sharing decision and your reasons, in line with the Trust Policy (CP12)

If there are concerns that a child may be at risk of significant harm or an adult may be at risk of serious harm, then follow the relevant procedures without delay.

Seek advice if you are not sure what to do at any stage and ensure that the outcome of the discussion is recorded.

Orange bold Italics relate to scenario specific responses

Addendum for Southern Health NHS Foundation Trust (HPFT)
Information Sharing protocols, guidance, policy, memorandums of understanding

CP 12.1 **Interagency Policy on Confidentiality & the Management of Service User Information, V5 (Agreement between HPFT, Hampshire Adult Services, Southampton Adult Services and Surrey & Borders Partnership NHS Foundation Trust**

CP 12.2 **Procedural Agreement between the Agencies on Arrangements for the Transfer and Management of Confidential Service User Information, Version 3**

CP 12.3 **Staff Practice Guidelines for Confidentiality and Information Sharing, Version 4**

Memorandum of Understanding for Potentially Dangerous People between HPFT and Hampshire Constabulary (January 2011)