Northamptonshire Safeguarding Adults Board

INFORMATION SHARING PROTOCOL

September 2019

Version 8 - Reviewed by Quality & Performance Sub Group – request for IGO signatories to be added	31st October 2018
Version 9.2 with signatures ratified with Board virtually	27th September 2019
Date of next review	October 2020

Introduction

This document, the Northamptonshire Safeguarding Adults Board Information Sharing Protocol, is a context specific protocol supporting the specific sharing of information for the purposes defined within the document.

This document is compliant with the general principles of information sharing as set out in guidance and legislation.

This document must underpin the exchange of information between agencies for the purpose of safeguarding adults at risk in Northamptonshire.

This document does not give agencies an automatic right to receive information or a mandate to provide information, but is instead a process for information sharing in cases in which it is suitable for information to be shared.

Sharing information about individuals between public authorities is often essential if adults at risk are to be kept safe or to ensure they receive appropriate services. The sharing of information must only happen when it is **legal** and **necessary** to do so and **adequate safeguards** are in place to protect the security of the information. Furthermore, where a death has occurred due consideration should be taken in respecting the dignity of an individual and their family.

As signatories to this protocol, it is agreed that Partners will cooperate fully with each other within the parameters of Data Protection legislation and other legislative restrictions.

1. Purpose of this Agreement

This document is specifically about sharing information for the purposes of safeguarding and promoting the welfare of adults at risk. Sharing of information between agencies and staff / practitioners working with adults at risk and their families / carers is essential. In many cases it is only when information from a range of sources is put together that individuals can be seen to be at risk of harm.

1.1 The Impact of sharing information

There may be anxieties about the legal or ethical restrictions on sharing information, particularly with other agencies. There should however be an awareness of the law and agencies and their staff / practitioners should comply with their relevant professional codes of conduct, organisational requirements and other relevant agency guidance. These rarely provide an absolute barrier to disclosure. A failure to pass on information that might prevent an adult at risk from being abused or a more serious tragedy could expose agencies / staff / practitioners to criticism in the same way as an unjustified disclosure.

Failure to share information may also have a significant impact on the wider community, such as regarding hate crime and adults at risk, honour based violence and on the records of personal information relating to the individual, location, circumstances of the alleged offence, previous criminal offences, health record, details of other members of the community, housing records, family relatives and providers of regulated services including statutory agencies.

A decision by a practitioner or member of staff whether to disclose information may be particularly difficult if a staff member / practitioner thinks it may damage the trust between themselves and the adult at risk. If such concerns arise advice should be sought from a senior colleague, designated professional, Information Governance / Data Protection Officer, Legal Personnel, if working in the NHS or local authority social services, this also includes the Caldicott Guardian.

2. Extent and Type of Information to be Shared

2.1 Type of Information to be shared

Partners will share any information relevant about an individual where that information is necessary for the safeguarding of the individual or others as detailed below.

The principle of proportionality will be applied to all sharing of information and the information to be shared will be considered on a case by case basis to ensure that only the minimum necessary information required is shared in each case.

2.2 Constraints on the use of the Information

Partners to this agreement undertake that data shared will only be used for the specific purpose for which it is disclosed, unless there is a legal obligation for the onward sharing of data.

The recipient of information under this agreement has an obligation under Data Protection Legislation ((i) the GDPR from 25 May 2018 (ii) The Data Protection Act 2018 and any secondary legislation as amended or updated from time to time (iii) any successor legislation to the GDPR or the Data Protection Act 2018) to consider the implications of further release of this information to any third party and prior to any further dissemination consent must be obtained from the originating Partner, except where there is a legal or safeguarding obligation.

2.3 Information Sharing Principles

- Must have lawful authority;
- Must be necessary;
- Must be proportionate;
- Must need to know;
- Must be accountable; and
- Must ensure the safety and security of the information shared.

2.4 The Golden Rules

It is a requirement of the Northamptonshire Safeguarding Adults Information Sharing Protocol that all agencies and staff / practitioners adhere to the Golden Rules for information sharing in all instances of information exchange. These are:

- Confirm the identity of the person you are sharing with
- Obtain consent to share if safe, appropriate and feasible to do so
- Confirm the reason the information is required, and that this is in line with the purpose the information is held for, or a legitimate legal purpose for sharing.
- Be fully satisfied that it is necessary to share or use anonymised data if possible
- Check with a manager / Data Protection Officer or seek legal advice if you are unsure
- Don't share more information than is necessary
- Inform the recipient if any of the information is potentially inaccurate or unreliable once you become aware of any inaccuracies
- Ensure that the information is shared safely and securely
- Be clear with the recipient how the information will be used
- Record what information is shared, when, with whom and why; and if you decide not to share record your reasons

2.5 What are the legal requirements which underpin the Golden Rules?

The decision whether to disclose information may arise in various contexts. There may be a concern about an adult at risk that might be allayed or confirmed if shared with another agency. A staff member / practitioner may be asked for information in connection with for example an assessment of an adult at risk's needs under s47 of the NHS and Community Care Act 1990 or an assessment under the Mental Health Act 1983. In all cases the main legislation which underpins the sharing of information in relation to adults at risk are:

- Common law duty of confidentiality;
- Data Protection Act 2018;
- Human Rights Act 1998;
- Freedom of Information Act 2000;
- Crime and Disorder Act 1998- Section 17 of the Crime and Disorder Act 1998 (as amended by the Police and Justice Act 2006 and the Policing and Crime Act 2009);

- The 2008 Entry Regulations duty to allow entry to local Healthwatch. The Legislation in Section 225 of the 2007 Act requires the Secretary of State for Health to make regulations to require certain persons to allow authorised representatives to "enter and view", and observe the carrying-on of activities on premises owned or controlled by the service provider;
- MCA Deprivation of Liberty Safeguards (DoLS) 2007; and
- Care Act 2014.

Each of these pieces of legislation has to be considered separately when deciding whether information can be shared. Other statutory provisions may also be relevant. But in general, the law will not prevent the sharing of information with other agencies / staff members / practitioners if:

- the public interest in safeguarding the adult at risk's welfare overrides the need to keep the information confidential; or
- disclosure is required under a court order or other legal obligation; or
- those likely to be affected consent

3. How the Information May be Used

3.1 Confidential Information

Confidential information is covered by the common law duty of confidence. It applies to any information that has been received or accessed in circumstances where it is reasonable to expect that the information will be kept secret or should only be shared with a limited number of specific people.

3.2 Sharing confidential information

The key principle is that any information confided should not be used for any other purpose or disclosed further except as originally understood by the confider or with their subsequent permission.

- The duty is not absolute and the disclosure of confidential information can be justified if:
- The information is not confidential in nature
- The person to whom the duty of confidence is owed has expressly authorised its disclosure
- Disclosure is required by a court order
- Disclosure is required by legislation or a legal obligation
- There is a serious overriding public interest as the information relates to:
    - Serious crime;
    - Danger to a person's life;
    - Danger to other people;
    - Danger to the community;
    - Serious threat to others, including staff;
    - Serious infringement of the law; and
    - Risk to the health of the person.

3.3 Maintaining confidentiality

All personal information acquired or held in the course of working with adults at risk should be treated as confidential. The confidential information each agency holds will be subject to the agency's confidentiality policy and must be stored securely in accordance with the agency's policy.

All health and social care staff and partner agencies have a common law duty of confidentiality within their work with adults at risk. They also have a duty to process personal information in line with the *Data Protection Act 2018* and to comply with the Caldicott principles. These are a set of requirements that ensure information regarding people who use services is treated with sensitivity to maintain its confidentiality. Information that has been provided in confidence and personal information should not usually be used or shared without consent from the subject and source of that information.

The above rule applies in almost all circumstances, but there are occasions where exceptions may apply. Where there is a perceived need to disclose personal / confidential information to another person or agency, it is necessary to consider carefully whether this is lawful in line with the common law, duty of confidence and the *Data Protection Act*. The reasons for disclosing personal / confidential information should always be recorded, and legal advice must be sought whenever there is doubt about a decision to disclose.

The following circumstances may arise where it may not be possible or appropriate to obtain consent to share information:

- the subject does not have the mental capacity to consent
- contacting the subject may, for example, jeopardise a serious criminal investigation or put someone in unacceptable risk
- the subject cannot be contacted within a reasonable timeframe - *the period of time considered reasonable will differ on a case-by-case basis depending on the urgency with which the information needs to be shared.*the subject has refused to give their consent
- the subject has refused to give their consent

If consent cannot be obtained due to the reasons stated above information may be shared without obtaining consent in exceptional circumstances where it is necessary for the information to be shared. Examples of what **may** override the duty of confidentiality include:

- The power of the Courts
- The power of certain Tribunals;
- A legislative requirement e.g. statutory assessment under the *Mental Health Act 1983* or to prevent:

    - Serious crime;
    - Danger to a person's life;
    - Danger to other people;
    - Danger to the community;
    - Serious threat to others, including staff;
    - Serious infringement of the law;
    - Breach of a legal obligation to supply the information;
    - The health of the person; or
    - Public health concerns.

It is essential that use, including recording, of such sensitive personal data adheres to the requirements of the protective marking policy i.e. all information irrespective of format being marked as 'Official '.

This classification is equivalent to 'NHS Confidential' as the NHS have a different protective marking policy. The confidential information each agency holds will be subject to the agency's confidentiality policy and must be stored securely in accordance with the agency's protocol. This includes the need for secure delivery of safeguarding information within and between other organisations.

3.4 Consent to share

Confidential or personal information may be shared if consent to share has been given by the confider or data subject. Unless there is another clear legal basis to share personal information, consent should be sought and properly recorded if it is safe and appropriate and feasible to do so. As a matter of routine good practice, a consent based approach is always the preferred option.

Where the confider or data subject (the individual about whom the data relates) has been assessed to lack mental capacity to give consent to the sharing of information then a Best Interests Decision should be made under the *Mental Capacity Act 2005* (as amended by *Mental Health Act 2007*. See *Mental Capacity Act 2005 Code of Practice Chapter 5*). The decision-maker should encourage participation of the individual, identify all relevant circumstances, find out the person's views (using an Independent Mental Capacity Advocate if required), avoid discrimination, whether the person may regain capacity and consult others. Any best interest assessment will ordinarily involve discussion with those close to the individual. In particular any person who has been named by the person to be consulted, close relatives/friends, any attorney appointed under a Lasting Power of Attorney for health and welfare or Enduring Power of Attorney or any Deputy appointed by the Court of protection to make decisions in relation to health and welfare.

In relation to domestic abuse however care has to be taken to ensure that anyone consulted who is close to the individual is in fact acting in his or her interests.

Although the past and present wishes of an incapacitated adult need to be taken into account when making a best interests assessment, they are not necessarily determinative. The decision needs to be made on the basis of the individual's current circumstances and needs, including, where necessary and appropriate, referral to appropriate authorities.

3.4.1 Recording and reviewing consent

A record including the date should always be made of any consent that has been given, refused or withdrawn. This should be referred to when information is shared to ensure that the scope of the consent is not exceeded. Unless there is another clear legal basis you can rely upon, consent should be re-sought if the information is to be used for a different purpose to that recorded or if there has been an unreasonable lapse of time since the consent to share was given. Consent should always be freely given, fully informed and unambiguous.

It should be noted that there may be circumstances where it may not be appropriate to seek consent from the individual such as the investigation of a crime and where sharing information may put the individual or the wider community a risk of serious harm to their mental or physical health.

3.4.2 Informed consent

Consent must always be informed. This means that the person giving consent must clearly understand all the available options and the consequences of them giving or withholding their consent.

3.4.3 Explicit or express consent

This is a clear and voluntary indication of consent to share specific information for one or more specified purposes.

3.4.4 Implied consent

This applies where it would be within the reasonable expectations of the data subject (the individual about whom the data relates) or confider that information may be shared without needing to obtain explicit consent. It is likely to apply where information is routinely shared and the data subject is aware of this or where information sharing is intrinsic to the purpose for which the data subject or confider supplied the information. For the avoidance of doubt implied consent should not be relied upon where informed consent is attainable.

3.4.5 Withdrawal or reconfirmation of consent

The confider or data subject may withdraw consent at any time and they should be made aware of this right. If consent is withdrawn, others with whom the information has been shared must be notified.

Consent must not be assumed to be open-ended. Confirmation of continued consent should be sought after a reasonable time according to individual circumstances and an expiry date for consent should be recorded.

In the event of a change in either the extent of information being sought, or the need to share with agencies not included in the original consent agreement, a revised consent should be sought unless the information may legitimately be shared without consent.

3.4.6 Sharing information without consent

It is not always safe, appropriate or feasible to obtain consent to share information. Circumstances where it may not be possible to obtain consent include:

- Where obtaining consent might be contrary to the public interest; including risk to the health of the person;
- The data subject / confider may be absent or not contactable;
- The data subject / confider may be permanently or temporarily incapacitated and has no appropriate representative; and
- The data subject / confider has withheld or withdrawn their consent.

Under the Common Law Duty of Confidence, the *Data Protection Act 2018* and the *Human Rights Act 1998* it is possible to disclose information without consent in the cases of serious public interest or in the best interests of an individual. Also under the *Crime and Disorder Act 1998* (as amended by the *Police and Justice Act 2006* and the *Policing and Crime Act 2009*) for Community Safety purposes.

Decisions regarding the disclosure of information without consent must always be made on a case-by-case basis. Any disclosure must always be proportionate and the minimum necessary to achieve the necessary objective.

If it is not possible to obtain consent before sharing information, the data subject / confider should be informed as soon as possible after the information has been shared, unless this would be inappropriate (e.g. cause serious harm; effect on ongoing investigation).

3.5 The impact of sharing or withholding information

Essentially, a decision to share information without consent rests on an assessment of the relative risk of disclosure and non-disclosure and a professional judgment on the most appropriate action that should be taken in the light of this assessment.

Two key questions are:

1. What if this information is not shared?
2. Who will be affected by this information being shared?

The former considers whether a negative impact is likely if the information is withheld. There will be a clear interest in disclosing information where there is an evident risk to the life or well-being of an individual which is accentuated or not addressed by not doing so; the protection of health, morals and the rights and freedoms of others; public safety; and the prevention of crime and disorder. If substantive, the public interest value may over-ride that of an individual's human rights.

The latter considers whether there is a disproportionately negative impact in information being made available, for example familial breakdown or personal risk resulting from unnecessary disclosure. Disclosure should be assessed for its potential impact on others who may be identifiable from the data such as witnesses, or staff who are involved in cases, or whose vulnerability makes their interests the over-riding consideration.

3.6 The Data Protection Act 2018 and Caldicott Principles (1997 & 2013)

The Caldicott Principles require that Heath and Social Care staff are professionally obliged to comply with those principles when processing person identifiable information. They should:

- Justify the purpose;
- Don't use person identifiable information unless absolutely necessary;
- Use the minimum necessary;
- Need to know basis;
- Be aware of your responsibilities;
- Understand and comply with the law; and
- The duty to share information can be as important as the duty to protect patient confidentiality.

The Data Protection Act is a key piece of legislation that provides a framework to processing of information that identifies living individuals. Remember that this legislation is not a barrier to share information but does provide a framework to share appropriately. This Act requires organisations to ensure that personal data is processed (i.e. obtained, held, used, disclosed and destroyed – this list is not exhaustive) in accordance with eight data protection principles, unless exemptions apply. It also grants individuals a right of access to their own personal information, unless exemptions apply.

The Health and Social Care Information Centre sets out the following rules in relation to treating confidential information with respect:

- Rule 1: Confidential information about service users or patients should be treated confidentially and respectfully;
- Rule 2: Members of a care team should share information when it is needed for the safe and effective care of an individual;
- Rule 3 Information that is shared for the benefit of the community should be anonymised
- Rule 4 An individuals right to object to the sharing of confidential information about them should be respected; and
- Rule 5 organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

Further information on these rules is available in the document "A Guide to Confidentiality in Health and Social Care "published by the Health and Social Care Information Centre.

The six data protection principles that relate to personal identifiable data are as follows:

1. Lawfulness, fairness and transparency;
2. Purpose limitation;
3. Data minimisation;
4. Accuracy;
5. Storage limitation;
6. Integrity and confidentiality (security); and

In addition data controllers shall be responsible for, and be able to demonstrate compliance with the principles ('accountability').

'Personal data' is defined under the applied GDPR 2016 as data which relate to an identifiable individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller. It is important to note that it includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual (an example of a data controller is Northamptonshire County Council).

This applies to anything that relates to a living individual in which the individual can be identified:

- Directly from the information (e.g. name and address); or
- From the combination of this information with other information that may be readily accessible (e.g. address but not name); and
- Which affects the privacy of the subject, whether in personal, family; or
- Business or professional life (Durant Case judgement 2003).

Special Categories of personal information as defined under the applied GDPR 2016 as personal data consisting of information as to:

- Racial or ethnic origin of the data subject;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- Genetic data
- Biometric data

- Data concerning health (includes physical or mental health or condition);
- Sexual life or sexual orientation;

The Six Data Protection principles of the applied GDPR 2016 must be complied with when processing any personal or special categories of personal data, unless an exemption applies.

Data protection legislation does not apply to information about people who have died. However, such information may still be sensitive, confidential or relate to individuals who are still alive. Information about people who have died may be shared under the provisions of this ISP and The Access to Health Records Act will cover this too.

Consent exemption – Schedule 1 Part 2 Paragraph 18 (safeguarding of children and of individuals at risk)

(1) This condition is met if—

(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—

(i) aged under 18, or

(ii) aged 18 or over and at risk,

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are—

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

(3) For the purposes of this paragraph, an individual aged 18 or over is “at risk” if the controller has reasonable cause to suspect that the individual—

(a) has needs for care and support,

(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and

(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.

Consent Exemption Schedule 2 Part 1 Paragraph 2: (sharing information for the purposes of Crime and Tax). This allows the disclosure of information without consent however, you must meet the requirements of the *Data Protection Act* and be in accordance with the Caldicott principles. This is considered on a case by case basis but does allow disclosure without consent under certain condition where there is a serious public risk. This includes:

- The prevention and detection of serious crime (murder, rape, GBH-grievous bodily harm); and
- The apprehension and prosecution of offenders who commit serious offences against the person.

It is essential in these cases when sharing information you do not have to inform the individual subject if it would prejudice these purposes. When sharing information for these purposes you do not have to comply with principles 1-5 of the DPA, but you must still meet a condition in schedule 2 and schedule 3 for sensitive personal information. For advice on managing requests under this exemption you should speak to your legal team or information compliance team.

3.7 The Human Rights Act 1998

Public Authorities must share information in accordance with the *Human Rights Act 1998*, which states that everyone has a right to respect for private and family life, his home and his correspondence.

A public authority may share information which may interfere with the above right if to do so 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, protection of health or morals or for the protection of rights and freedom of others.

3.8 Freedom of Information Act 2000

Most signatories to this agreement are public authorities and therefore subject to Freedom of Information Act 2000 (FOI). Where a signatory is not a public authority this section will not apply to that organisation or information held by that organisation.

The FOI grants a right of access to any information held by public authorities, unless there are valid legal reasons why this information should not be disclosed. It is intended to promote a culture of openness and to facilitate a better public understanding of how public authorities carry out their duties, the reasoning behind their decisions, and how public money is spent.

The FOI does not interfere with the public authority's obligation to protect personal or confidential data, nor does it inhibit an individual's right to access their own personal information, as prescribed under the Data Protection legislation.

Public Authorities have an obligation under the *FOI* and Data Protection legislation to consider requests from any person or organisation for access to any information that they hold. This may include safeguarding adult information, including the minutes of meetings and information shared by any other party in connection with safeguarding adult investigations.

Public Authorities will not release information if any of the exemptions defined in *FOI* apply. The exemptions include personal information, information supplied in confidence (this is because the information would originally have been provided to a healthcare practitioner or social worker in confidence, and we consider this duty of confidentiality to extend beyond death), and information for which a claim to legal professional privilege can be maintained.

There may be circumstances where information relating to safeguarding adult investigations is released, but only where it is appropriate to do so. A situation where information may be released would be where a case has been concluded with no concerns regarding the safety of those involved, and where permission has been received from all relevant parties for the disclosure of the information. However, advice should always be sought from Legal, Data Protection, Information Governance and Caldicott Guardian as appropriate.

3.9 Crime and Disorder Act 1998

The *Crime and Disorder Act 1998* introduced measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in the local area.

Section 115: establishes a gateway (the power) to disclose information, which is central to the Act's partnership approach. It must be remembered that this is a power and not a duty meaning you must still meet the requirements of the *Human Rights Act*, *Common Law* and the *DPA* (this gateway can be used to meet one condition in schedule 2, but you are still required to meet a condition in schedule 3 for sensitive personal information). The Police have an important and general power at common law to disclose information for the prevention, detection and reduction of crime. However, some other public bodies which collect information may not previously have had power to disclose it to the Police and others. This section therefore puts beyond doubt the power of any organisation to disclose information to Police authorities, local authorities, probation committees, health authorities, or to persons acting on their behalf, so long as such disclosure is necessary or expedient for the purposes of this Act. These bodies also have the power to use this information.

It is to be noted that there is no requirement to exchange information, merely permission to do so.

The purposes of the Act broadly cover the prevention and reduction of crime and the identification or apprehension of offenders.

3.10 Safeguarding adults meetings and notes

In order to safeguard an adult at risk or other vulnerable people, it may be necessary to share confidential information at safeguarding adults meetings. It is the responsibility of the Chair of that meeting to request any relevant information and to secure the agreement of the relevant parties to sharing this information.

The Chair of the safeguarding meeting will ensure that a confidentiality statement is made at the start of the meeting and all parties understand their responsibilities in respect of confidentiality.

Exchange may be verbal or written however data protection principles must still apply with attendees only being present where it is appropriate for them to share the information.

Attendees at safeguarding adults meetings will be asked to sign an attendance list which will confirm their individual compliance with the protocol.

Notes taken at safeguarding meetings will be marked 'OFFICIAL'. Only those people who have been invited to the meeting will receive copies of the notes and they must be filed in the confidential / safeguarding adults section of any case file / electronic record.

In all circumstances consent to use and disclose copies of notes / minutes of meetings must be sought from the chair of the meeting.

Any requests for access to the notes of safeguarding adult meetings must be considered on a case by case basis under the Freedom of Information Act 2000 and / or the *Data Protection Act 2018*, but information will only be disclosed if it is appropriate to do so. For further advice, contact should be made with the Data Protection Officer or Freedom of Information officer from the relevant organisation or contact can be made with the Information Commissioner.

If an organisation wishes to disclose confidential information, permission i.e. consent, must be obtained in writing from the initial owner of the information (unless there is a legal obligation to share). If this may not be appropriate, then prior advice should be sought from above the Data Protection / Freedom of Information officer from the relevant organisation or, contact can be made with the Information Commissioner.

It is recommended that information relating to safeguarding adult issues should be retained on case files / electronic records for 30 years. Information should then be reviewed and if agreed only then securely disposed.

3.11 The Care Act 2014

The Care Act is a key piece of legislation for social care and safeguarding. The Act set out for the first time, in law, the role and purpose of Safeguarding Adult Boards (SABs), making these statutory bodies, and made safeguarding adults a statutory duty of local authorities. While doing this it gave safeguarding adult boards specific powers to request information. It also made it a duty of local authorities, and their partners, to co-operate with each other in what it terms both general and specific cases relating to individuals' care and support. This duty to co-operate will apply to the sharing of information along with other forms of co-operation.

Section 45 deals specifically with the supply of information to SABs. In outline if an SAB makes a request for information, the person to whom the request is made must comply if two mandatory conditions are met, and one of two other conditions are met. The mandatory conditions are that:

1. The request is made for the purpose of enabling the SAB to exercise its function.
2. The request is made to someone whom the SAB considers likely to have information relevant to the SAB's function (i.e. safeguarding adults).

One of the following two conditions must also be met:

3. The information relates to the person to whom the request is made, a function or activity of that person, or a person in respect of whom that person exercises a function or an activity.

4. The information has already been supplied to another person subject to an SAB information request, or is derived from such information.

The information will be supplied to the SAB or another person specified by the SAB in the information request.

In some cases these requests will be made of SAB members, but in other cases these requests will be directed to agencies that don't have a seat on the SAB. The duty to supply the information is the same in both cases.

Sections 6 & 7 outline how the co-operation between partners should work, when it applies, and under what circumstances an agency may decline to co-operate. This co-operation is a general duty and does not apply specifically to information sharing, but information sharing will certainly fall within its remit. The purpose of this co-operation is to:

1. Promote the well-being of adults with care and support needs, and carers, in the authority's area.
2. Improve the quality of care and support for adults, and support for carers, in the authority's area.
3. Smooth the transition between children's and adult services.
4. Protect adults with care and support needs who are experiencing, or at risk of, abuse or neglect.
5. Identify lessons to be learnt from cases where adults with care and support needs have experienced serious abuse or neglect and apply those lessons.

Those required to co-operate include: local authorities, district councils, NHS bodies, local offices of the Department for Work and Pensions, the police, prison services and probation services. There may be other organisations a local authority decides it should be co-operating with such as care providers, housing associations, independent hospitals and regulators.

Co-operating in specific cases Where a local authority or partner requests co-operation from another partner or authority, in relation to a specific case, the partner or authority must co-operate unless doing so would be incompatible with their own duties, or have an adverse effect on the exercise of their functions. The request to co-operate should be made in writing, referring to the Care Act provision. If the partner or authority declines to comply with the request, this also should be done in writing, giving their reasons for not co-operating. The response should be given in a reasonable timescale.

Advocacy A key element of the Care Act is the right to advocacy. Adults must have access to either independent advocates or appropriate adults, where there are substantial difficulties engaging with certain social care process such as assessment or safeguarding enquries. Where there are others lawfully representing adults, information must also be shared with these advocates so they can effectively support and involve those they advocate for, through the safeguarding, assessment or review process.

4. Security and Data Management

4.1 Secure information exchange methods

It is important that information is shared safely and only shared with the intended recipient. The information should show the originator's details, including organisation name (where applicable) and date.

4.2 Email

Due to the timeframes within the Safeguarding Adults Procedures it may be necessary to use email for the circulation of notes of safeguarding meetings and reports. Care should be taken to anonymise witness and alleged perpetrator identifying information, e.g. by using initials. The risks in relation to using email is acknowledged, however, its use has been agreed to ensure timely exchange of information to those recipients who are not in possession of a secure encrypted email account or do not have email encryption software. This applies to the creation and delivery of Safeguarding meeting notes despatched by the chair. In all such circumstances, the document must be password protected (if encryption is not available). This applies to the delivery of Safeguarding meeting notes dispatched by the chair and any members of the team involved in the process.

When password protection is applied to a document the password must be communicated via an alternative medium (eg by telephone) to minimise the risk of the password being compromised.

Where an organisation has access to Government Connect / GCSX (or equivalent), this facility must be used. It is a secure network between central government and every local authority in England and Wales. It is part of the wider Government Secure Intranet (GSi) and provides connectivity to nearly all central government departments as well as the NHS and the police.

4.3 Fax

This is only secure if the person who requires the information is waiting by the receiving fax machine to receive the document immediately or the fax machine is located in a secure "safe haven". Do not assume this will always be the case, ensure the recipient is waiting for the fax before it is sent. A fax header sheet (that does not contain any personal information) must be transmitted first with the information itself sent only after a confirming response has been received. A record of the transmission must be retained.

Faxes should only ever be used as a last resort.

4.4 Postal or Courier Services

Postal Services can never be fully secure and are not recommended unless secure email is not possible. If post is to be used, ensure that you use an envelope that will show if it has been tampered with (preferably inside another envelope), and is marked 'Private and confidential addressee only'. It is recommended that if the Post Office system is used, Recorded, Special, Business mail Secure or Royal mail tracked service be chosen, as this allows the mail to be tracked. A courier service could alternatively be used, depending on the sender's requirements or sensitivity of the information.

4.5 Personal exchange

Paper copies of information can be exchanged in person provided that both the information holder and the recipient take appropriate measures to ensure that it cannot be read by anyone who does not have a legitimate reason to do so. Paper copies should be kept secure at all times.

4.6 Verbal Exchange

This is only secure if it is not repeated to anyone who is not authorised to hear it, or overheard when exchanged or discussed e.g. in a busy office or during a conference phone call. If information is exchanged verbally in a manner where it is not recorded at the time, the exchange should be validated and confirmed in writing as soon as possible.

4.7 Disposal of Data/information

At the end of its use (for copy information) or agreed retention period information should be securely disposed of in line with internal procedures. Where information has been shared, and the receiving organisation is not the data controller, authority of the originating organisation should be sought before destruction takes place.

4.8 Storage

All organisations must ensure that reasonable steps are taken to ensure the security of data – this includes the management of data when in transit between organisations. Each signatory to this agreement is expected to have an information security framework that documents how information will be kept secure. This will be made available to partners on request.

4.9 Security Breaches

In addition to compliance with the Golden Rules (see section 2 above), once the individual recipient has been verified and validated then the information shall be disclosed securely.

Any concern or allegation of an unauthorised loss of information / disclosure of information or breach of confidentiality / principle of the *Data Protection Act* 2018 must be reported as soon as possible using the relevant internal reporting channels within the appropriate organisation. Any level 3 breach (as defined in the Data Security and Protection Incident Reporting Tool) will be reported to the Department of Health and Social Care and the ICO.

4.10 PREVENT

Prevent is 1 of the 4 elements of CONTEST, the government's counter-terrorism strategy. It aims to stop people becoming terrorists or supporting terrorism. The Prevent strategy:

- Responds to the ideological challenge we face from terrorism and aspects of extremism, and the threat we face from those who promote these views; and
- Provides practical help to prevent people from being drawn into terrorism and ensure they are given appropriate advice and support.

works with a wide range of sectors (including education, criminal justice, faith, charities, online and health) where there are risks of radicalisation that we need to deal with

For the avoidance for doubt the safeguarding elements of the PREVENT programme are included in the remit of this protocol.

4.11 The Role of Healthwatch

Local Healthwatch will take on the work of the Local Involvement Networks (LINks) and will represent the views of people who use services, carers and the public on the Health and Wellbeing boards set up by local authorities. They will also provide a complaints advocacy service to support people who make a complaint about services and report concerns about the quality of health care to Healthwatch England, which can then recommend that the Care Quality Commission take action.

Due to the advocacy nature of their role there may be times when information may need to be shared from Healthwatch to other statutory bodies. Such sharing is covered by the remit of this protocol where it relates to a safeguarding matter.

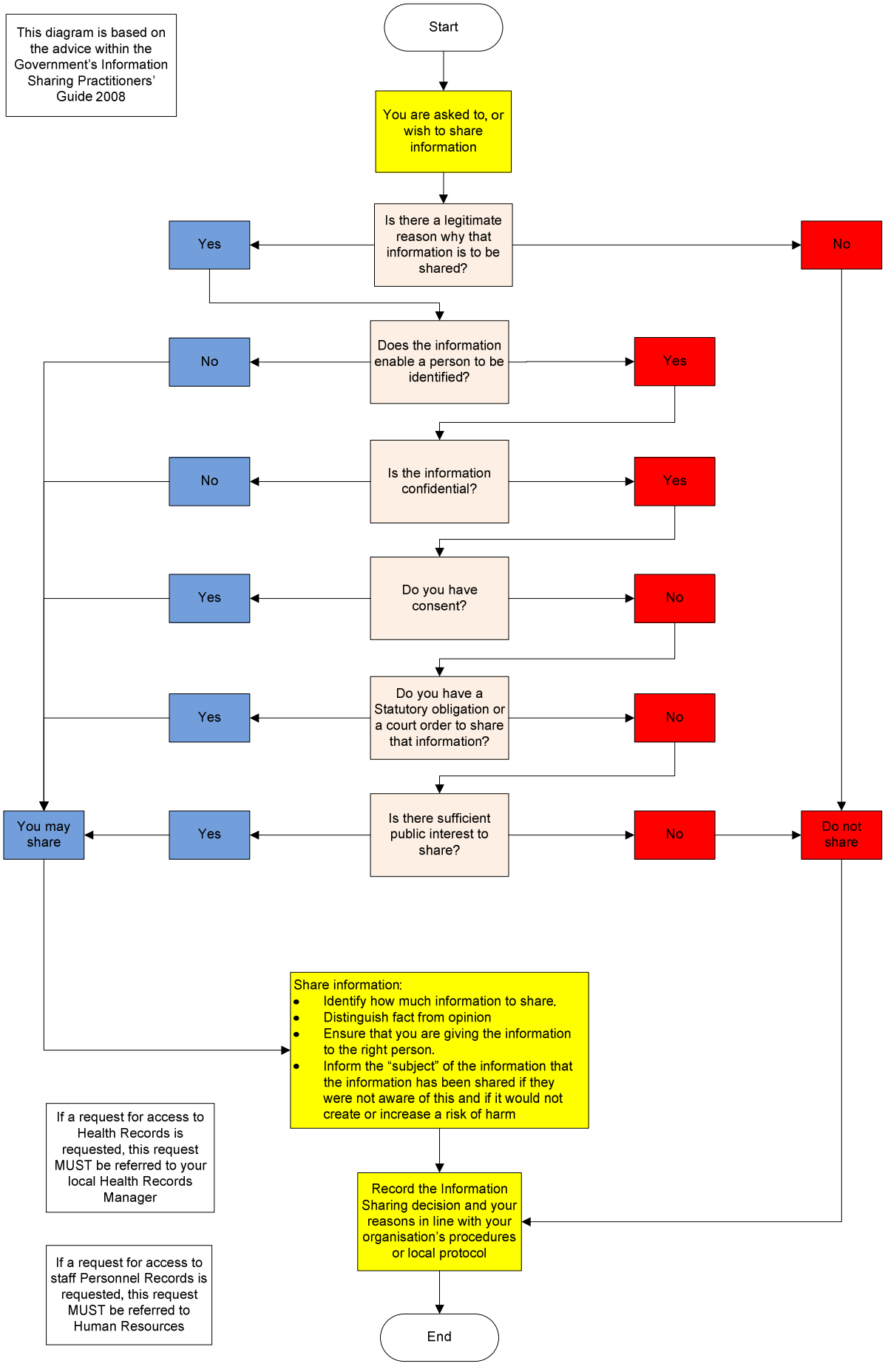
The relationship between Healthwatch and the Safeguarding agencies will be reviewed as this develops and any changes required to the protocol will be agreed by the SAB.

5. Implementation and review

The Northamptonshire Safeguarding Adults Board is responsible for the implementation and review of this protocol. This protocol will be reviewed at least every two years.

All signatories to this ISP are responsible for ensuring that their organisations comply with the legislative framework of the MAISP protocol and working with policies that adequately reflect the secure processing of data. Each organisation may use their own templates for information sharing. Northamptonshire County Council, Northamptonshire Police and NHS Corby and NHS Nene Clinical Commissioning Groups forms are included in the appendices below:

Decision Making in Information Sharing V 1.0



Appendix II

Northamptonshire Safeguarding Adults Board

Safeguarding Information Sharing Form – Access to Records Request

(Ref: Information Sharing Protocol for Safeguarding Adults – October v8 2018)

Safeguarding Information Sharing Request			
For the attention of:		**Date of request:**	
Person Requesting:			
Title:			
Organisation/Agency:			
Contact Details:			
Email address:			
Method of Request (tel/letter/email/fax/in person):			

Subject of this Information Request			
Individual's Name:			
Any other name:			
Current address:			
Postcode:			
Previous address:			
Postcode:			
D.O.B.:	/ /	**NHS No. (if known):**	
NCC ID No. (if known):			

Consent by the Individual - *See section 3.4 of the Information Sharing Protocol*		
Has the individual given informed consent?	☐ Yes (attach proof)	☐ No
If no, give reason for pursuing the request without consent below:		

Reason for/nature of request - *See section 2 and 3.11 of the Information Sharing Protocol (Care Act requests)*
Type of Information requested:
Which timescale/date(s) does the information request relate to?
What will the information be used for, why is it needed?

Is this a section 45 request (SAB information request)?
Is this a section 7 request (co-operation in specific cases)?

Response to Information Sharing Request	
To whom was the response given?	
Date of the response:	
Name of senior manager authorising/not authorising:	
Title:	
Agency:	
Contact Details:	
Reason for sharing/not sharing:	
If not shared, what action was taken as a result?	

Type of Information Shared (no details)		
Brief description:		
With whom was the information shared?		
Date information was shared?		
Are any restrictions/limitations placed on the use of information shared?	☐ Yes	☐ No
If yes, what are they?		

Signature of person sharing/not sharing the information:	
Date:	
Signature of manager authorising the decision:	
Date:	

DISCLOSURE OF INFORMATION TO THE POLICE
(Data Protection Act 2018, Schedule 2, Part 1 (2))

Our reference		Date	29 October 2018
To:	.		

I am making enquiries which are concerned with :

- ☐ A missing person
- ☐ National security
- ☐ The apprehension or prosecution of offenders
- ☐ Fraud
- ☐ Prevention or detection of crime
- ☐ The vital interests of the data subject

Information required:

.

The reasons the information is required:

.

and possibly for other crime enquiries and administration purposes.

I confirm that the personal data requested is required for the purposes stated above and failure to provide the information will, in my view, be likely to prejudice that purpose. In authorising the request for this data, the Authorising Officer has considered the issues and proportionality under the Human Rights Act 1998.

Requesting officer	.	Rank/Role	Detective Chief Inspector Safeguarding Adults
Authorising officer		Rank/Role	Detective Chief Inspector Safeguarding Children
Signature			

Address	Northamptonshire Police Headquarters Wootton Hall Northampton NN4 0JQ	Tel	03000 111 222 extn: 345875
		Fax	
Email	richard.tompkins@northants.pnn.police.uk		

Corby Clinical Commissioning Group

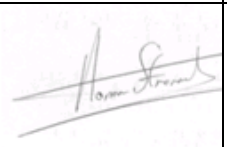
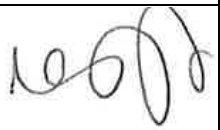
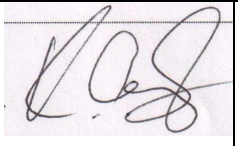
Nene Clinical Commissioning Group

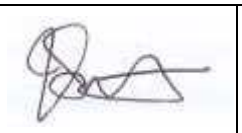
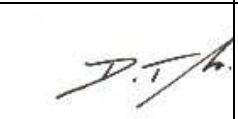
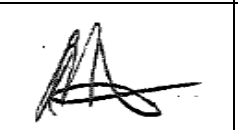
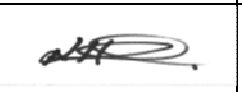
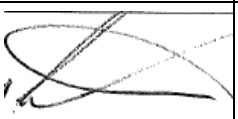
CCG Information Request Template			
Details of Board/Community Safety Partnership/Other Requesting Information	**Please details auspices of legislation/guidance**	**Purpose and Justification**	
Details of concern and time period:			
Individual(s) records to be accessed:	**Has consent been obtained:**	**If no consent obtained please detail authority sanctioning access:**	
Name **DOB**	**Yes / No**		
Name **DOB**	**Yes / No**		
Name **DOB**	**Yes / No**		
Name **DOB**	**Yes / No**		
Date:	**Role:**	**Name:**	**Signed:**

Parties to the Protocol – Appendix V

This Information Sharing Protocol defines the arrangements for processing data between the agencies listed below for the purposes of safeguarding adults.

There are other reasons for agencies to share information which are not covered by this agreement such as the obligation for agencies to share information with their regulators for the purpose of assurance.

NSAB Information Sharing Protocol				
Organisation	**Officer**	**Position**	**Signature**	**Date**
The Bedfordshire, Northamptonshire, Cambridgeshire and Hertfordshire Community Rehabilitation Company (BeNCH CRC)	Emma Osborne	Regional CEO		04.03.2019
Borough Council of Wellingborough	Liz Elliott	Managing Director		01.08.2019
Corby Borough Council	Norman Stronach	Chief Executive		18.07.2019
NHS Corby & NHS Nene Clinical Commissioning Groups	Dr Sanjay Gadhia Darin Seiger	Caldicott Guardian	 	07.05.2019 (received 17.07.19)
Daventry District Council	Maria Taylor	Executive Director (Community)		04.03.2019
East Midlands Ambulance Service NHS Trust	Janette Kirk	Data Protection Officer		17.12.2018
East Northamptonshire Council	Julia Smith	Head of Customer and Community Service		15.02.2019
HMP Onley	Keith Cummins	Head of Offender Management		19.12.2018

HMP Ryehill	Jodyne Smith	Offender Managament Unit Manager		05.03.2019
Kettering Borough Council	Martin Hammond	Executive Director		21.12.2018
Kettering General Hospital NHS Trust	Leanne Hackshall	Director of Nursing & Quality		20.12.2018
Northamptonshire Association of Registered Care Homes (NorARCH)	Darrell Byrom	Chairman		09.01.2019
Northampton Borough Council	David Taylor	Data Protection Officer		20.12.2018
Northampton General Hospital NHS Trust	Sally Shocklidge	Data Protection Officer		07.05.2019
Northamptonshire County Council	Jill Buchanan Huck	Director of Operations ASC		28.02.2019
Northamptonshire Fire & Rescue Service	Kelvin Hallen	Head of Service Delivery		08.01.2019
Northamptonshire Healthcare Foundation Trust	Julie Shepherd	Director of Nursing, AHP's & Quality		08.02.2019
Northamptonshire Police	Trina Kightley-Jones	Data Protection Officer		09.01.2019
National Probation Service - Northamptonshire Probation Trust	Denise Meylan	Head of LDU		10.01.2019
St Andrew's Healthcare	Lisa Cairns	Head of Nursing		28.02.2019
South Northamptonshire Council	Louise Aston	Information Governance Manager		09.01.2019