Police information requests to NHS Organisations, GPs and other healthcare providers in respect of potential homicide investigation, proof of life enquiries and more general enquiries to trace missing persons

Notes:

NHS organisations are willing to share information based on seriousness of case and appropriate police authority level but are concerned about fishing expeditions in comparison with genuine requests in potential homicide cases.

The NHS uses a common reference number, the NHS number, across all care delivery organisations for patient safety reasons. The expectation is that this number is not held routinely on police information systems. However, in the context of an episode of emergency care, it may be used to support identification.

Process considerations:

- Authority levels – applications should be authorised by a substantive chief inspector or superintendent
- Application for information must contain sufficient information to describe seriousness of case (the justification for the request)
- Applications need to demonstrate proportionality, legality, accountability, necessity and justification
- Use email title bars to describe, in summary, the contents of request email (eg. proof of life enquiry– missing from Kilmarnock since April 2017)
- Application should contain a request for both positive and negative returns
- Request for any relevant information to be passed to a specified contact in police force (eg. originator's name, address, telephone numbers and, preferably, a group e-mail address)
- Preferred templates should be used if available (note, there is no specific national template)
- For Police Scotland, the request should set out need for completion of any additional documentation to satisfy the Criminal Procedure (Scotland) Act 1995
- Caldicott Guardians are involved in authorising (or establishing procedures for) the release of information to the police.

Legal basis for sharing information:

In setting out why it would be lawful for a NHS organisation to provide information with the police[1] under the GDPR and DPA 2018 in relation to a missing person, a NHS organisation would be able to provide information in relation to a missing person to the police.

Article 6(1) of the GDPR sets out the lawful processing bases. An NHS organisation can lawfully provide information in relation to a missing person to the police on the basis of:
(d) processing is necessary in order to protect the vital interests of the data subject, and
(e) processing is necessary for the performance of a task carried out in the public interest.

There is a need to express why an individual's vital interests are at stake and that simply saying that a missing person is 'high risk' is unlikely to be convincing. In this regard, see Schedule 1 (Part 2) paragraph 18 of the DPA 2018[2]. Paragraph 18 provides an exception from the processing of special

[1] The answer is the same regardless of whether the requesting police force is Police Scotland, an England and Wales Police force, the NCA, or a police force in another country.

[2] Schedule 1 (Part 2) paragraph 18 DPA 2018:

(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 subparagraph (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.

category personal data, including health records, where it is necessary for reasons of substantial public interest namely for the purpose of safeguarding of children and individuals at risk (see Article 9(1) and (2)(g) of the GDPR in conjunction with section 10(1)(b) and (3) of the DPA 2018).

Where a police force requests information from an NHS organisation for a missing person, the NHS organisation can rely on this exemption to provide an individual's health records to the police under Article 9(2)(g). The NHS organisation should be able to rely on a police force's assessment that a missing person is 'high risk' and that they are therefore 'at risk' (per para 18(1)(b)). It may help if requests include details / criteria in respect of when an individual would be assessed as a 'high risk' missing person, so that NHS organisations and UKCGC can be satisfied that the criteria are met. This exception could be met in many missing persons cases even if they are not 'high risk', and if it wishes the NHS organisation could always seek further information from the police force to satisfy itself that the criteria in paragraph 18 is met.

It logically follows that, if an NHS organisation can rely paragraph 18 as an exception to Article 9 of the GDPR and provide health care records of a missing person to the police then, an NHS organisation must be able to provide other non-sensitive information to the police under Article 6 of the GDPR (such as details of their address or confirmation that the individual has had treatment without stating the details of the treatment).

Thus an NHS organisation can lawfully provide appropriate and proportionate information, including health care records, of a missing person to the police that is necessary for the purpose - but usually not the whole record. Whether the NHS organisation should provide the information is another question, and of course an issue for them. However, we should be arguing that a NHS organisation *should* provide some information, for example confirmation as to whether a patient has registered with them. For these reasons, we expect the Caldicott Guardian to authorise any information given to the police in the potential homicide investigation, proof of life enquiries and more general enquiries to trace missing persons.

In the event that information is available and the individual is alive and has capacity, the individual (or guardian if the individual does not have capacity) will be informed of any disclosures made about them.

For completeness, if a missing persons investigation becomes a criminal investigation then the NHS organisation could rely on the basis under Article 6(1)(e) of the GDPR and the crime and taxation exemption under Schedule 2 (part 1) paragraph 2.

The Criminal Procedure (Scotland) Act 1995 is about Scottish criminal procedure – not whether information can lawfully be provided to Police Scotland. This Act does not require, nor provide any basis for, an organisation (in Scotland or England and Wales) to provide information to Police Scotland. Instead it sets out the procedure that must be followed to enable Police Scotland to enter documentary evidence that it receives from organisations (in Scotland or England and Wales) into evidence in Scottish criminal proceedings. An 'enquiry response document' is drafted in such a way such that it complies with procedural requirements in this Scottish Act, so that if required Police

Scotland can introduce the information provided in the response into evidence. Information can lawfully be provided by anybody to Police Scotland in the format requested, or an alternative format, provided the General Data Protection Regulations / Data Protection Act 2018 is complied with.

The common law duty of confidentiality is satisfied because the public interest in sharing is sufficient to support the *limited* information sharing involved. Caldicott Guardians should refer to the GMC confidentiality guidance (S50-76) "Disclosures for the protection of patients and others" (https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality/disclosures-for-the-protection-of-patients-and-others) to ensure only necessary and proportionate information is shared with the police. Any further sharing within the NHS, e.g. to support a referral, is subject to normal NHS information sharing practice. The common law duty of confidentiality will be satisfied when information is shared:

- where there is a clear statutory obligation to share confidential information; or
- with the consent of the individual concerned; or
- where it is in the best interests of an individual who lacks the capacity to consent to the sharing; or
- where the public interest served by sharing the minimum information needed to satisfy a purpose outweighs both the duty of confidentiality owed to an individual and the public interest in services being seen to be provided on a confidential basis.

In addition there are a number of legal gateways that enable sharing of information, for example:

Court orders - These include Police and Criminal Evidence Act, 1994 applications and applications in respect of coroners' investigations (Coroners and Justice Act 2009).

Safeguarding - Information must be shared for child or vulnerable adult safeguarding purposes (for example, under s.47 Children Act 1989).

The Caldicott Principles

In 2012, following concerns about how patients' information was being used in the NHS, a committee was established under the chairmanship of Dame Fiona Caldicott to investigate. In the resulting report seven Caldicott Principles were identified. These were re-published in 2016 in the National Data Guardian for Health and Care Review of Data Security Consent and Opt Outs. These principles do not provide a legal basis for sharing but are a useful summary of how to proceed.

CP1	**1. Justify the purpose(s)** Every proposed use or transfer of personal-confidential data within or from an organisation should be clearly defined, scrutinised and documented with continuing uses regularly reviewed, by an appropriate guardian.

CP2	**2. Don't use personable identifiable information unless it is absolutely necessary** Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
CP3	**3. Use the minimum necessary personal confidential data** Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a function to be carried out.
CP4	**4. Access to personal confidential data should be on a strict need-to-know basis** Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.
CP5	**5. Everyone with access to personal confidential data should be aware of their responsibilities** Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff are made fully aware of their responsibilities and obligations to respect patient confidentiality.
CP6	**6. Comply with the law** Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.
CP7	**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.