A Consultation on Information Sharing Agreements between NHS Scotland Boards and Police Scotland

August 2019

Scottish Government
Riaghaltas na h-Alba
gov.scot

Responding to this Consultation
We are inviting responses to this consultation by 30th October 2019.

Please respond to this consultation using the Scottish Government's consultation hub, Citizen Space (http://consult.gov.scot). Access and respond to this consultation online at https://consult.gov.scot/cmo/information-governance . You can save and return to your responses while the consultation is still open. Please ensure that consultation responses are submitted before the closing date of 30th October 2019.

If you are unable to respond using our consultation hub, please complete the Respondent Information Form to:

CMO Taskforce
Scottish Government
GWR
St Andrews House
Edinburgh, EH1 3DG

Handling your response
If you respond using the consultation hub, you will be directed to the About You page before submitting your response. Please indicate how you wish your response to be handled and, in particular, whether you are content for your response to published. If you ask for your response not to be published, we will regard it as confidential, and we will treat it accordingly.

All respondents should be aware that the Scottish Government is subject to the provisions of the Freedom of Information (Scotland) Act 2002 and would therefore have to consider any request made to it under the Act for information relating to responses made to this consultation exercise.

If you are unable to respond via Citizen Space, please complete and return the Respondent Information Form included in this document.

To find out how we handle your personal data, please see our privacy policy: https://beta.gov.scot/privacy/

Next steps in the process
Where respondents have given permission for their response to be made public, and after we have checked that they contain no potentially defamatory material, responses will be made available to the public at http://consult.gov.scot. If you use the consultation hub to respond, you will receive a copy of your response via email.

Following the closing date, all responses will be analysed and considered along with any other available evidence to help us. Responses will be published where we have been given permission to do so. An analysis report will also be made available.

Comments and complaints
If you have any comments about how this consultation exercise has been conducted, please send them to the contact address above or at CMOTaskforce.secretariat@gov.scot.

Scottish Government consultation process
Consultation is an essential part of the policymaking process. It gives us the opportunity to consider your opinion and expertise on a proposed area of work.

You can find all our consultations online: http://consult.gov.scot. Each consultation details the issues under consideration, as well as a way for you to give us your views, either online, by email or by post.

Responses will be analysed and used as part of the decision making process, along with a range of other available information and evidence. We will publish a report of this analysis for every consultation. Depending on the nature of the consultation exercise the responses received may:

- indicate the need for policy development or review
- inform the development of a particular policy
- help decisions to be made between alternative policy proposals
- be used to finalise legislation before it is implemented

While details of particular circumstances described in a response to a consultation exercise may usefully inform the policy process, consultation exercises cannot address individual concerns and comments, which should be directed to the relevant public body.

Table of Contents

Data Protection Impact Assessment (DPIA) Questionnaire for

Sharing Personal data between Health and other public agencies with regards to the provision of forensic medical and healthcare services provided to people those individuals who have been victims of rape, sexual assault and sexual abuse.

V0.14

[Date :31 July 2019]

DOCUMENT CONTROL SHEET

Key Information

Title	Sharing Personal data between Health and other public agencies with regards to the provision of forensic medical and healthcare services to people who have been victims of rape and sexual abuse.
Date Published/ Issued	
Date Effective From	
Version/ Issue Number	0.14
Document Type	Data Protection Impact Assessment
Document Status	DRAFT
Author	
Owner	
Approvers	
Contact	
File Name	

Revision History

Version	Date	Summary of Changes
0.1	07/01/19	Initial Working Document
0.2	11/03/19	Updated with consent and populated.
0.3	19/03/19	Consolidation of DPIA following meeting
0.4	26/03/19	Update to legal basis for research, included additional special category data.
0.5	29/04/19	Comments from EB, text updated with suggestions. Flow Diagram flattened. All flow descriptions composited. Additional Guidance document V0.1
0.6	02/05/19	Replaced patient with service user. Renamed flow as decision tree
0.7	15/05/19	Replaced service user with individual. Updated decision tree with holders for child and adults with incapacity processes. Added additional decision trees for request. Added basic data flow diagrams. Added appendix with SOPs needed for

		the DPIA. Comments on legal basis and risk areas updated.
0.8	28/05/19	Old comments removed. Duplicate risk removed. BMA changed to GMC
0.9	28/06/19	Updated decision tree with adult and child clinical pathways. Expanded Information flows. Spelling corrections. All comments removed
0.10	02/07/19	Updated from feedback
0.11	04/07/19	Updated formatting- Font set to Arial with minimum 12pt. Repagination as required. Non-functioning URLS removed, Removal of URLS from section 6 for clarity. Remaining functional URLS listed in full.
0.12	11/07/19	Updated GDPR legal bases for consistent wording with ISA
0.13	23/07/19	Updated from feedback from CLO and Solicitors
0.14	30/07/19	Updated following proof read for spelling and grammatical errors

Approvals

Version	Date	Name	Designation

About the Data Protection Impact Assessment (DPIA)

The DPIA (also known as privacy impact assessment or PIA) is a tool, which is used to identify, assess and mitigate any actual or potential risks to privacy created by a proposed or existing process or project involving the use of personal data. It helps us to identify the most effective way to comply with our data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow us to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. Failing to manage privacy risks appropriately can lead to enforcement action from the Information Commissioner's Office (ICO), which can include substantial fines.

A DPIA is not a 'tick-box' exercise. Consultation may take a number of weeks to complete, so make sure that key stakeholders are engaged early, and that you have enough time prior to delivery to iron out any issues.

Carrying out a DPIA is an iterative process. Once complete, a review date within the next 3 years must be set. Should a specific change in purpose, substantial change in service or change in the law occur before the review date, the DPIA must be re-done.

The ICO code of practice on conducting privacy impact assessments is a useful source of advice.

The DPIA is just one specific aspect of risk management, and therefore feeds into the overall risk management processes and controls in our organisation.

Is a DPIA required?

If the process or project that you are planning has one or more of the aspects listed below then you must complete a DPIA at an early stage.

		YES/NO
1.	The work involves carrying out a ***systematic and extensive evaluation*** of people's personal details, using ***automated processing (including profiling).*** Decisions that have a ***significant effect*** on people will be made as a result of the processing. <u>Includes:</u> Profiling and predicting, especially when using aspects about people's work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements Processing with effects on people such as exclusion or discrimination <u>Excludes:</u> Processing with little or no effect on people	No
2.	The work involves carrying out ***large scale*** processing of any of the ***special categories*** of personal data, or of ***personal data relating to criminal convictions and offences.*** <u>Includes:</u> • racial or ethnic origin data • political opinions data • religious or philosophical beliefs data • trade Union membership data • genetic data • biometric data for the purpose of uniquely identifying a person • health data • sex life or sexual orientation data • data which may generally be regarded as increasing risks to people's rights and freedoms e.g. location data, financial data • data processed for purely personal or household matters whose use for any other purposes could be regarded as very intrusive <u>To decide whether processing is ***large scale*** you must consider:</u> • the number of people affected by the processing, either as a specific number or as a proportion of the relevant population • the volume of data and/or the range of different data items being processed	No

		YES/NO
	• the duration or permanence of the processing • the geographical extent of the processing activity	
3.	The work involves carrying out ***large scale*** and ***systematic monitoring*** of a ***publicly accessible area.*** Includes processing used to observe, monitor or control people.	No
4.	The work involves ***matching or combining datasets*** e.g. joining together data from two or more data processing activities performed for different purposes and/or by different organisations in a way that people would not generally expect; joining together data to create a very large, new dataset.	No
5.	The work involves processing personal data about ***vulnerable groups.*** This includes whenever there is a power imbalance between the people whose data are to be used e.g. children, the mentally ill, the elderly, asylum seekers, and the organisation using their personal data.	Yes
6.	The work involves ***significant innovation*** or use of a ***new technology.*** Examples could include combining use of fingerprint and face recognition for improved physical access control; new "Internet of Things" applications.	No
7.	The work involves transferring personal data across borders ***outside the European Economic Area.***	No
8.	The work involves processing that will ***prevent people from exercising a right*** or using a service or a contract e.g. processing in a public area that people passing by cannot avoid.	No

Step One – Consultation Phase

Consult with all stakeholders about what you wish to do as early as possible in the process. Stakeholders will normally include:

- key service staff e.g. those who will be managing the process.
- technical support, especially if a new system is involved. This may involve the relevant IT supplier.
- information governance advisors e.g. Caldicott Guardian, Information Security Officer, Data Protection Officer.

Sometimes it will be necessary to consult with service users. This will be particularly relevant if the change in process will change how they interact with our NHS Board, or what information is collected and shared about them.

Early consultation will ensure that appropriate governance and security controls are built into the process as it is being designed and delivered, rather than being 'bolted on' shortly before the change is launched.

Step Two- DPIA drafting

The responsibility for drafting a DPIA will normally sit with the service area that 'owns' the change. However, all stakeholders will have an input. Depending on the nature and complexity of your proposal, more than one service area and/ or Information Asset Owner (IAO) may be the owner(s).

Step Three- Sign-off

[NHS Board may need to also add in here specific, local/ administrative details on how DPIAs should be carried out and recorded in their organisation e.g. links with the Information Asset Register, mailboxes to use etc]

When a DPIA has been fully completed, it must be submitted for formal review by an appropriate IG professional/ the Data Protection Officer. They will review the DPIA to ensure that all information risks are fully recognised and advise whether appropriate controls are in place. The Data Protection Officer will decide, where the DPIA shows a high degree of residual risk associated with the proposal, whether it is necessary to notify the ICO. It may be necessary to inform and/or involve the Board's Senior Information Risk Owner (SIRO) as part of this risk assessment and decision-making.

Once reviewed, the DPIA will need to be signed off by the Information Asset Owner(s) (IAOs), normally a head of service.

1. **<u>What are you trying to do and why? - give (or attach separately) a high level summary description of the process, including its nature, scope, context, purpose, assets e.g. hardware, software used, data flows). Explain the necessity and proportionality of the processing in relation to the purpose(s) you are trying to achieve.</u>**

Provide for the exchange of information between NHS Scotland, the Police Service of Scotland, Social Services (public agencies), for the purposes of provision of Healthcare and Forensic Medical Services for Victims of Rape, Sexual Assault and Sexual Abuse with a view to supporting their care and case management, including the collection, preservation and sharing of forensic evidence.

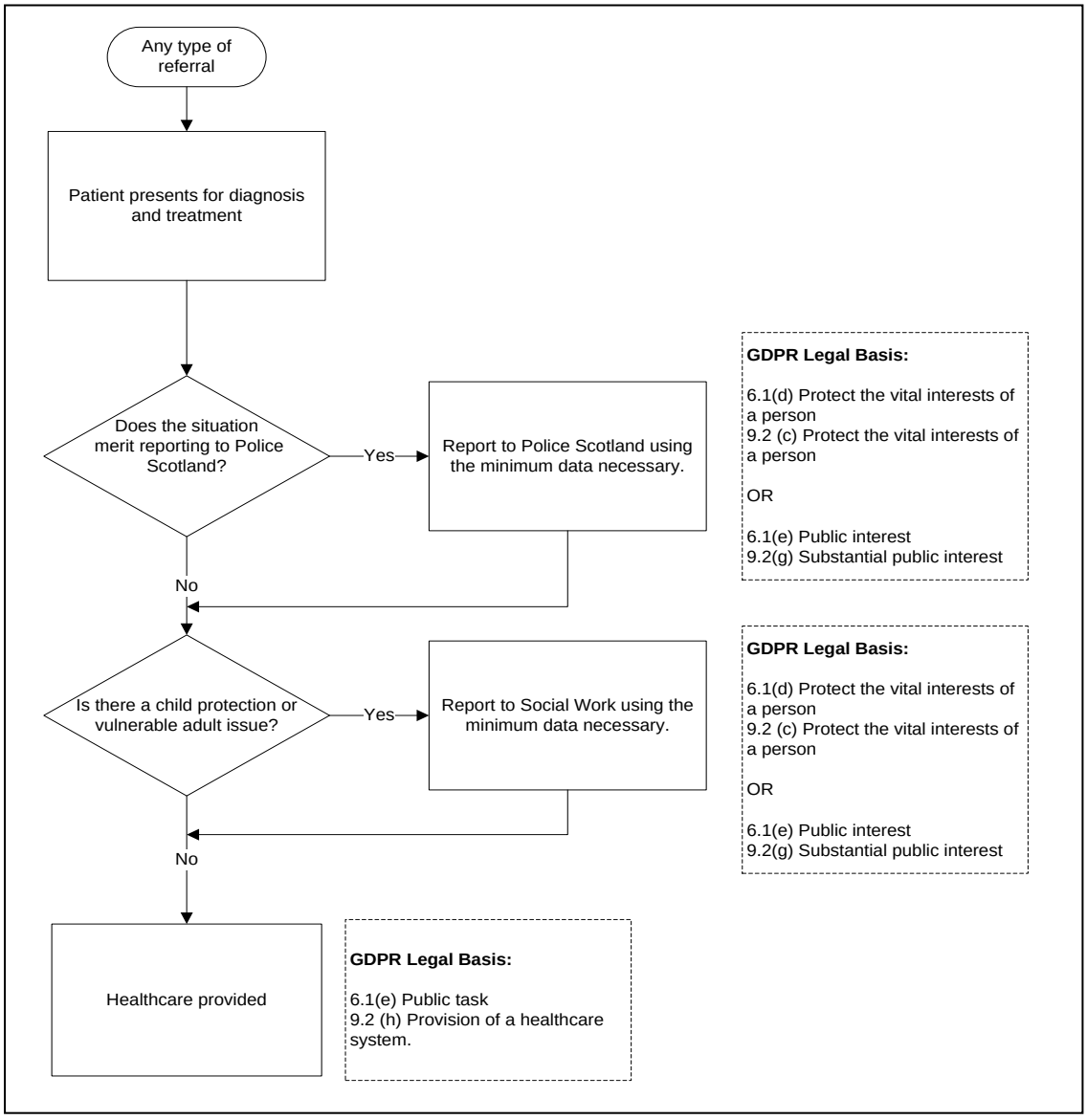
The exchange of information can be for the following purposes:

- support healthcare for those in the care of the Police
- support healthcare for those not reporting to the Police
- support the collection and sharing of forensic evidence
- support integrated care and case management
- support consistency in the sharing of information with the Police Service of Scotland and social work
- support community continuity of care
- support onward referral to appropriate services and agencies
- support the provision of services and the continuous improvement of services
- achievement of better outcomes for service users receiving care
- safety and wellbeing of service users who may be in need of care and protection (including children and young people)
- investigation, prevention and detection of crime
- preservation of personal and community safety
- assessment of need at individual and community level
- management and planning of services
- supporting the Taskforce vision of consistent, person centred, trauma informed care for all victims of rape, sexual assault and sexual abuse in Scotland

How processing sits with NHS Scotland.

The legal basis used to process personal and special category information for the day to day operation of NHS Scotland is given below. The “business as usual” model is out of scope of this DPIA, but is provided for information to give context for the provision of Healthcare and Forensic Medical Services for Victims of Rape and Sexual Assault.

Business as Usual Legal Bases



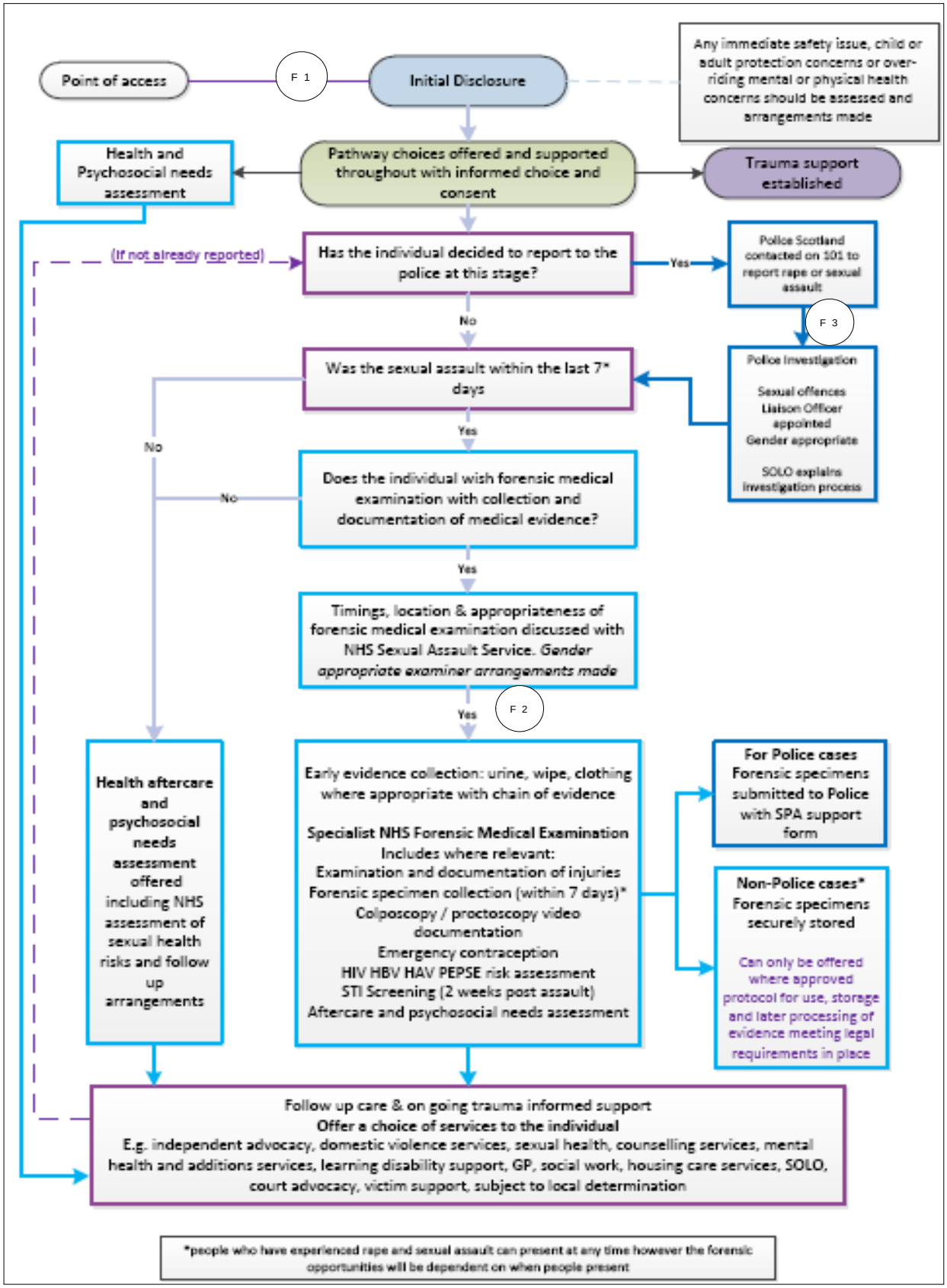
Information Flows

In each pathway the information flows covered by this DPIA are denoted by a circle with a reference number.

Eg. Information Flow 1 is denoted by the symbol 

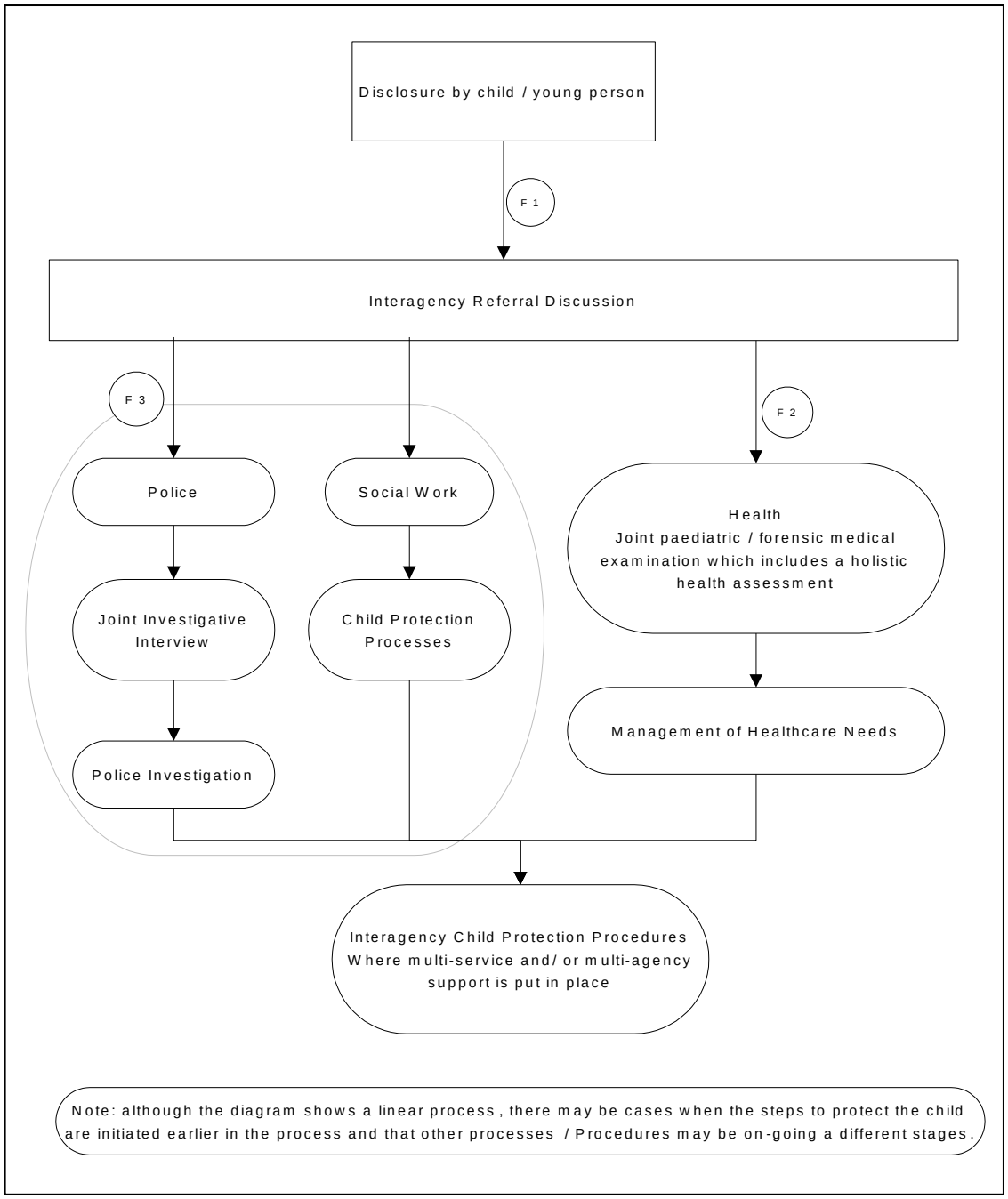
Adult Clinical Pathway

The adult clinical pathway is shown for information only. It gives context for where personal and special category information will be shared. It is these information flows that are the focus of this DPIA rather than the clinical pathway.

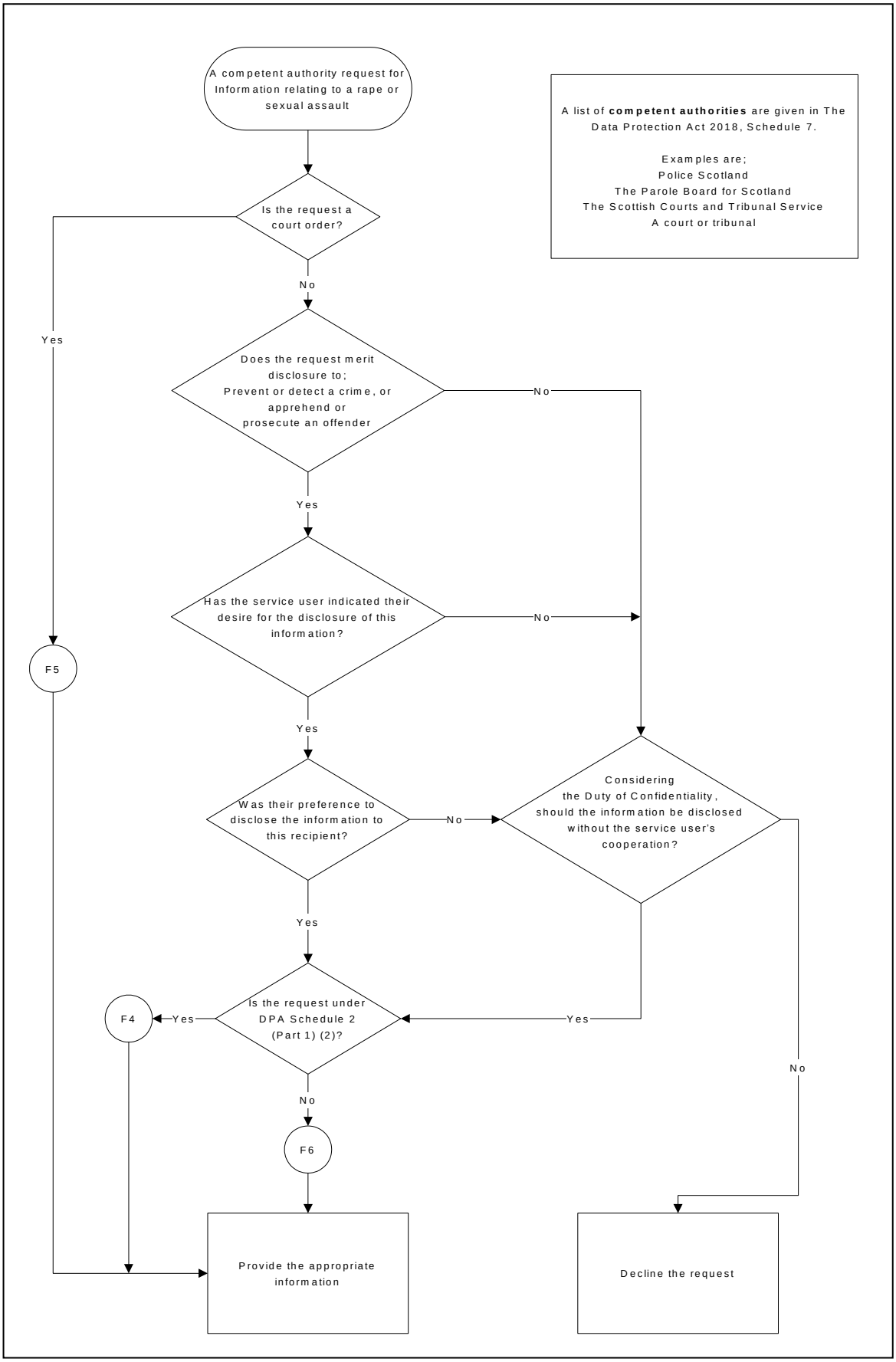


Child / Young Person Clinical Pathway

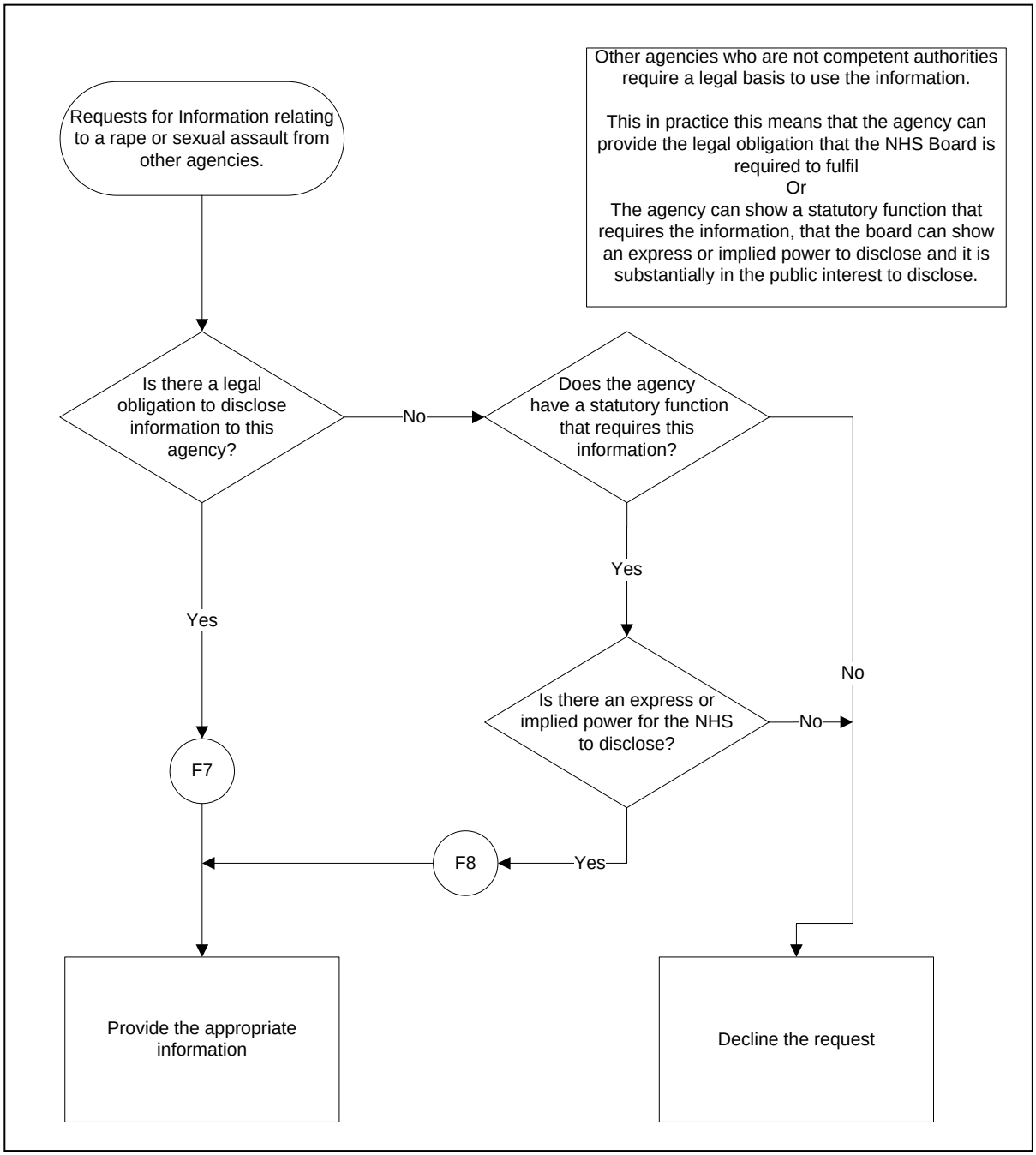
The child / young person clinical pathway is shown for information only. Again, to give context for where in the pathway personal and special category information will be shared. It is these information flows that are the focus of this DPIA rather than the clinical pathways.



NHS to a Competent Authority Disclosure Pathway

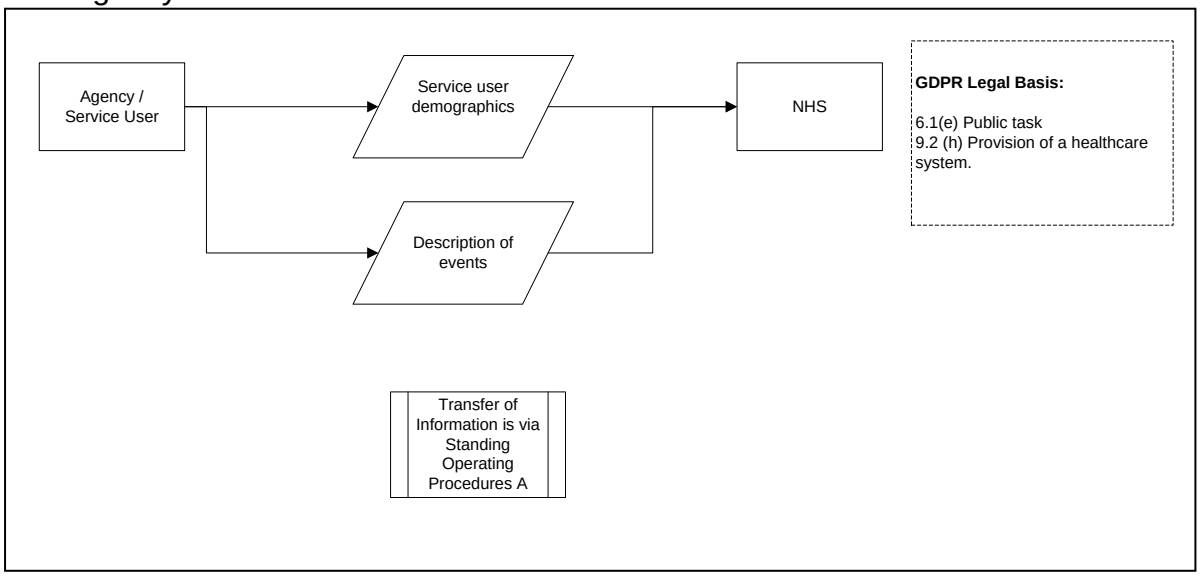


NHS to Other Agencies Disclosure Pathway

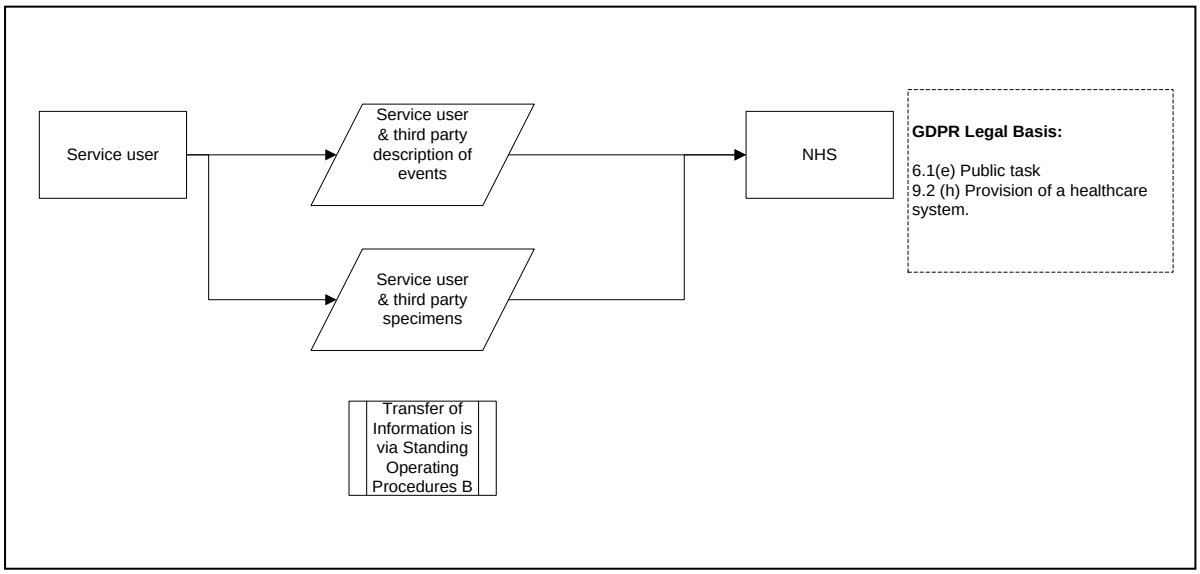


Information Flows

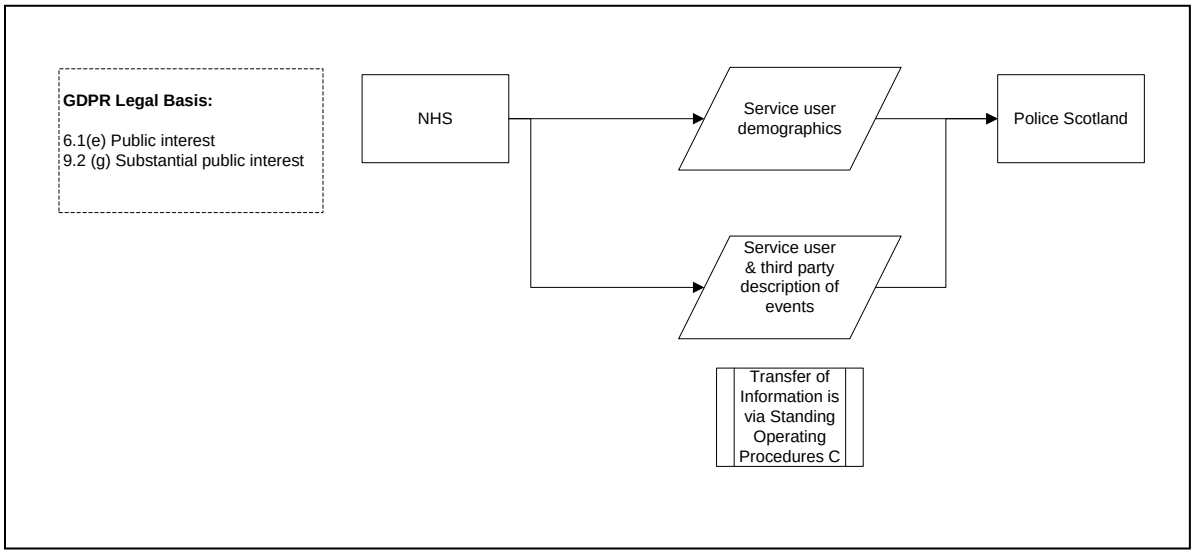
F1 - Agency / Service user to NHS



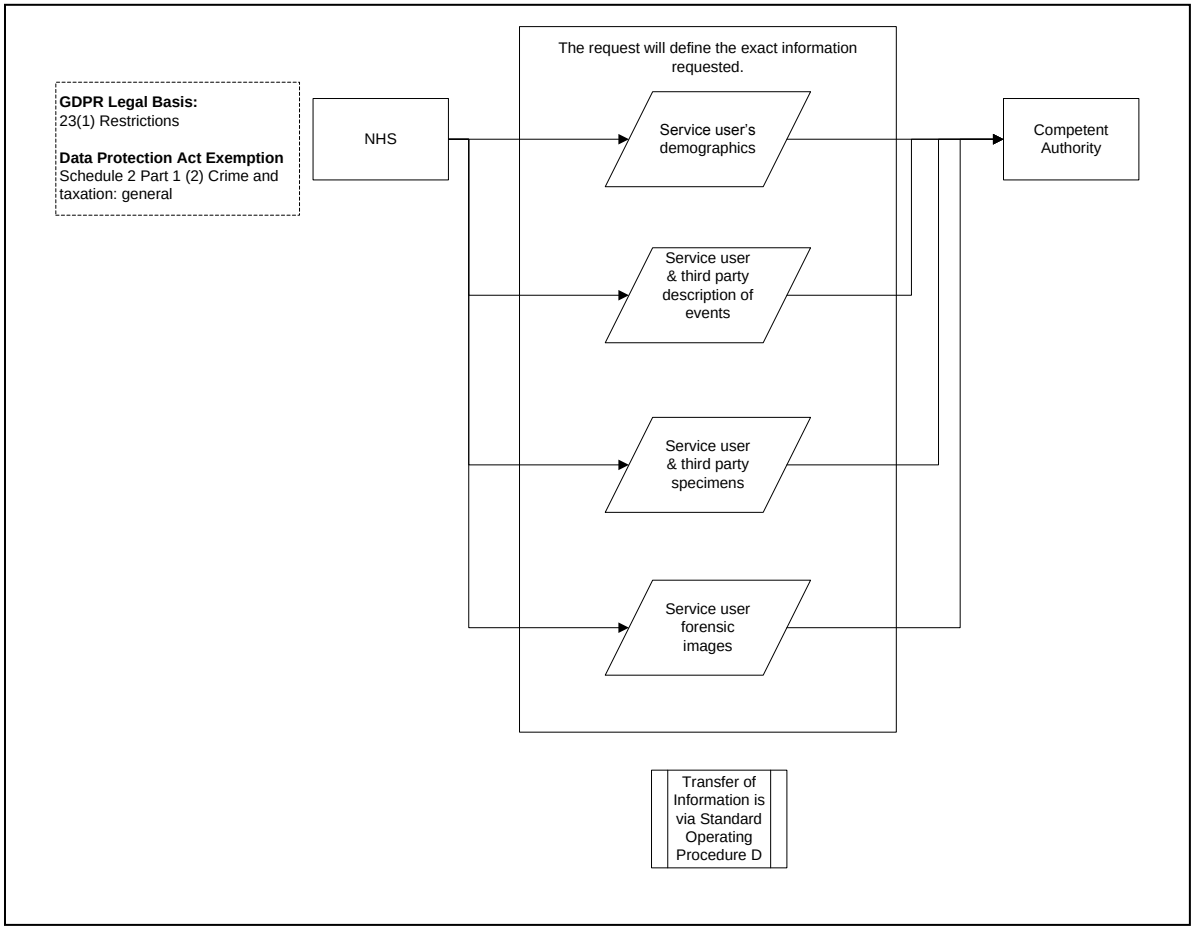
F2 - Service user to NHS



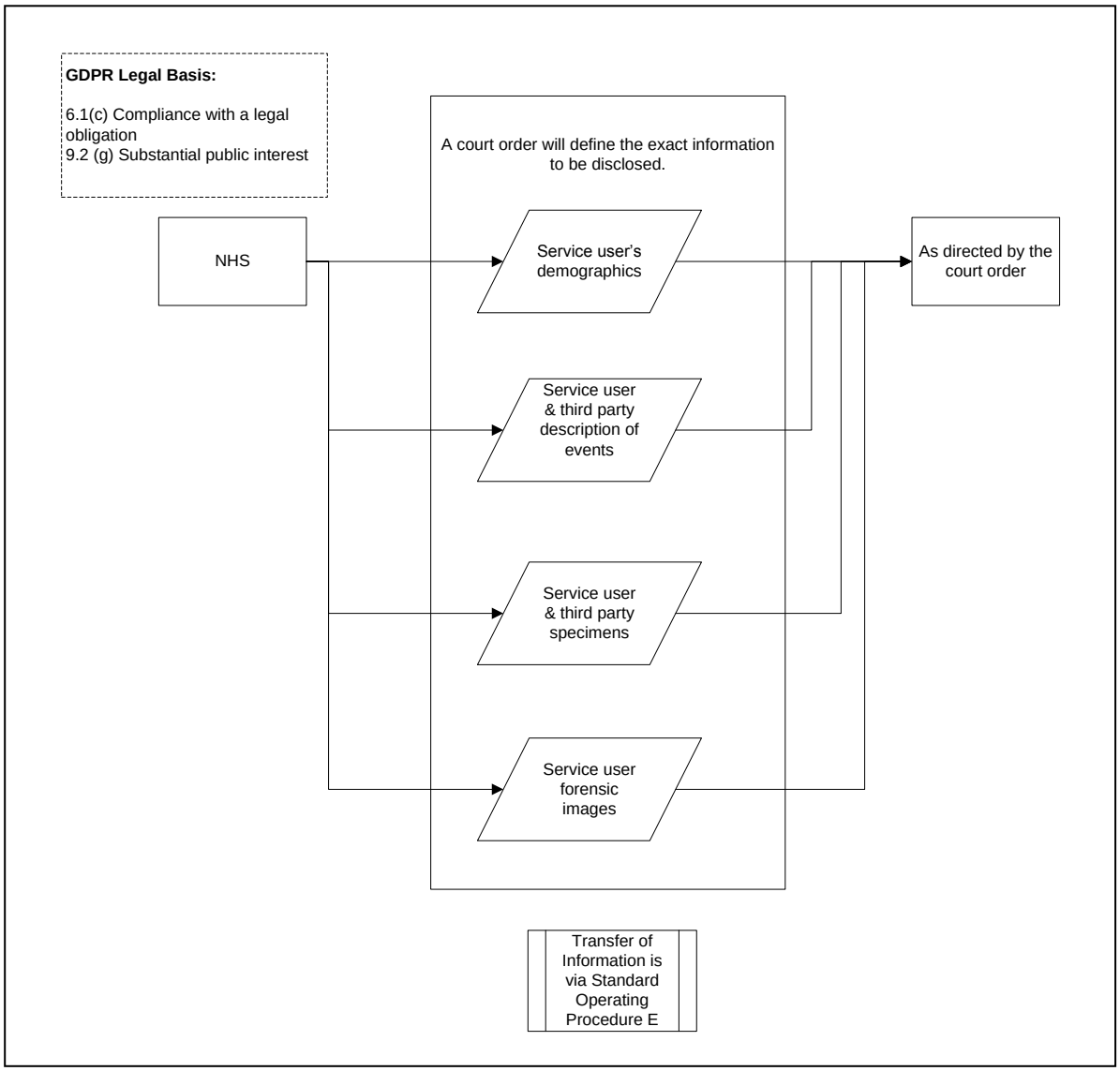
F3 - NHS to the Chief Constable of the Police Service of Scotland



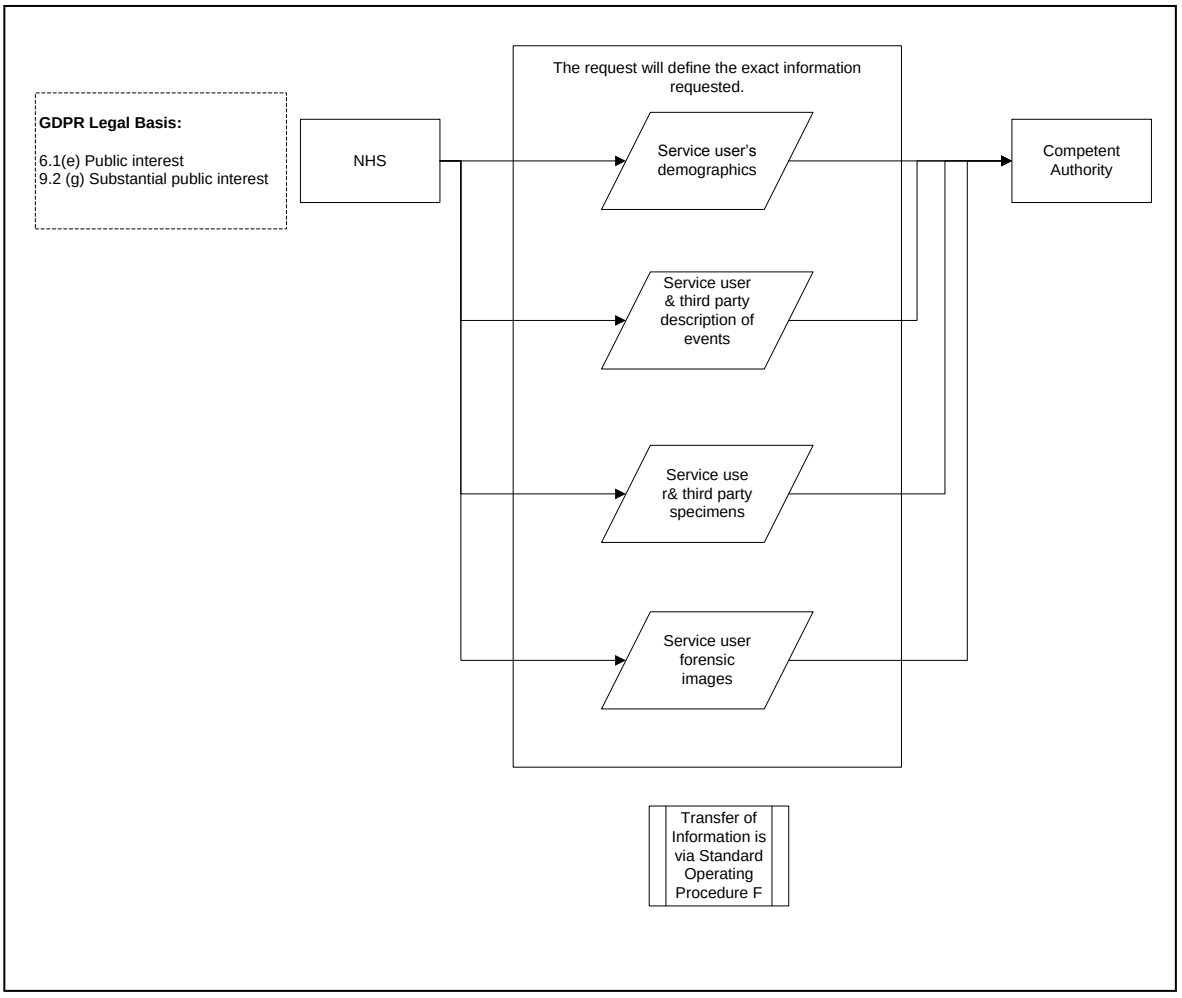
F4 - NHS to competent authority



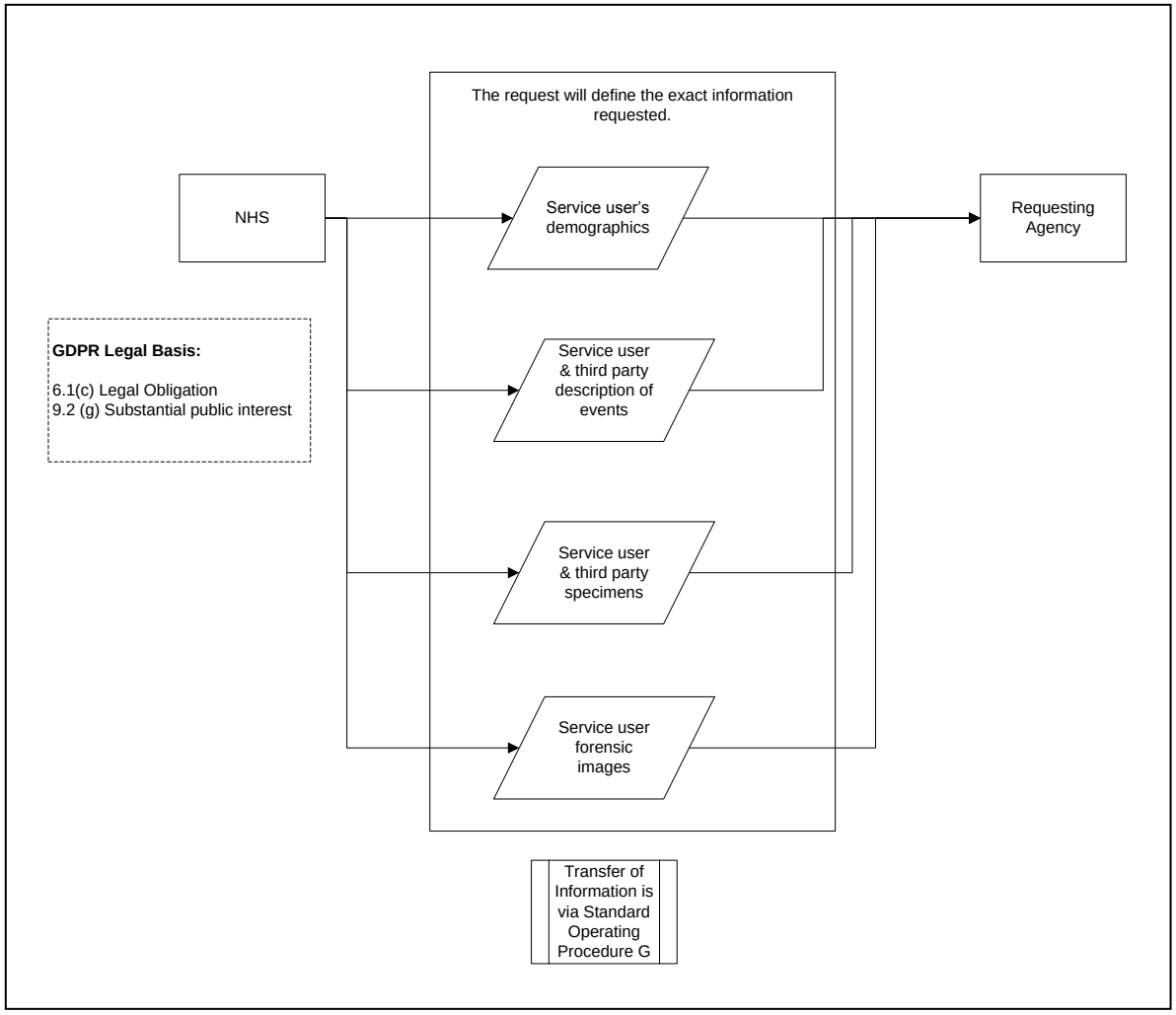
F5 - NHS compliance with a court order



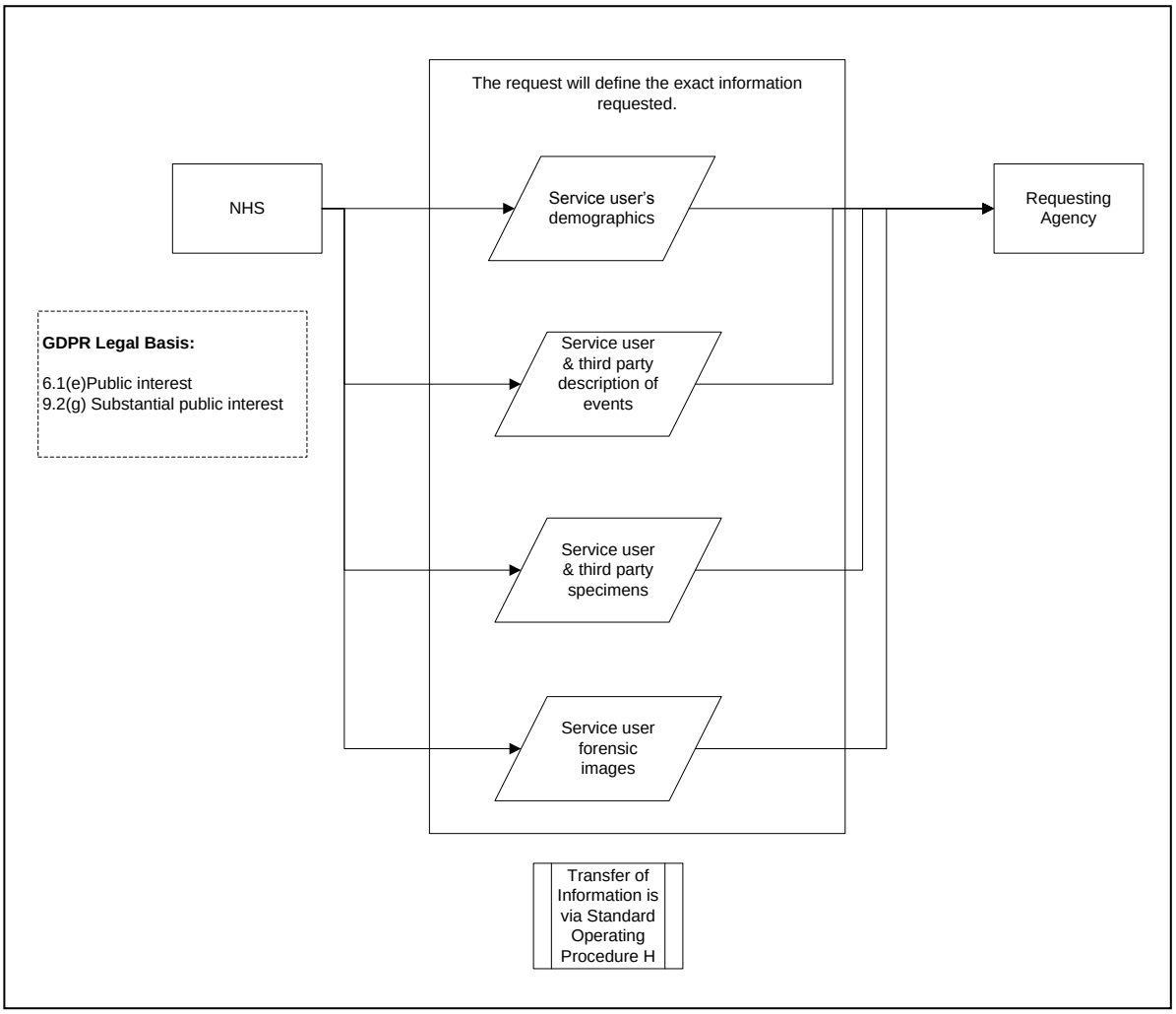
F6 NHS to competent authority



F7 NHS to other Agency



F8 NHS to other Agency



2. What personal data will be used?

Categories of individuals	Categories of personal data	Any special categories of personal data [see Guidance Notes for definition]	Sources of personal data
Service user	Health Record	Health Sexual life Sexual orientation	Provided by Service user NHS
Service user	Specimens	Health Criminal Genetic	Provided by Service user
Service user	Description of events	Health Sexual life Criminal	Provided by Service user, Police Service of Scotland, NHS
Service user	Forensic Images	Health Sexual life Criminal	Provided by Service user, Police Service of Scotland, NHS
Service user	Demographic	Racial or ethnic origin Religious or philosophical beliefs	Provided by Service user, Police Service of Scotland, NHS
Third Party	Specimens	Health Criminal Genetic	Provided by Service user
Third Party	Description of events	Health Criminal	Provided by Service user, Police Service of Scotland, NHS

3. **<u>What legal condition for using the personal data is being relied upon? [see Guidance Notes for the relevant legal conditions]</u>**

Legal condition(s) for *personal data* [see Guidance Notes]	**Legal conditions for any *special categories of personal data* [see Guidance Notes]**
All Circumstances Provision of health care, treatment and management of a health or social care system (NHS) General Data Protection Regulation Article 6(1)(e)	**All Circumstances** Provision of health care, treatment and management of a health or social care system (NHS) General Data Protection Regulation Article 9(2)(h) Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1) General Data Protection Regulation Article 9(2)(j)
Advising the Police Service of Scotland when they are not aware General Data Protection Regulation Article 6(1)(e)	**Advising the Police Service of Scotland when they are not aware** General Data Protection Regulation Article 9(2) (g). DPA Schedule1 Part 2 (10) Preventing or detecting unlawful acts.
Compliance with a court order General Data Protection Regulation Article 6(1)(c)	**Compliance with a court order** General Data Protection Regulation Article 9(2)(g) DPA Schedule 1 Part 2 (6) Statutory etc and government purposes.
Transfer of material, samples or information to a competent authority General Data Protection Regulation Article 23(1) Data Protection Act 2018: Exemption Schedule 2 (2): Crime and taxation: general. or General Data Protection Regulation Article 6(1)(e)	**Transfer of material, samples or information to a competent authority** General Data Protection Regulation Article 23(1) Data Protection Act 2018: Exemption Schedule 2 (2): Crime and taxation: general. or General Data Protection Regulation Article 9(2)(g) DPA Schedule 1 Part 2 (10) Preventing or detecting unlawful acts.
Transfer of information to other	**Transfer of information to other**

Legal condition(s) for *personal data* [see Guidance Notes]	**Legal conditions for any *special categories of personal data* [see Guidance Notes]**
agencies General Data Protection Regulation Article 6(1)(c) or General Data Protection Regulation Article 6(1)(e)	**agencies** General Data Protection Regulation Article 9(2)(g) DPA Schedule 1 Part 2 (6) Statutory etc and government purposes. or General Data Protection Regulation Article 9(2)(g) DPA Schedule 1 Part 2 (10) Preventing or detecting unlawful acts.

4. **Describe how the personal data will be collected, used, transferred and if necessary kept up to date – may be attached separately.**

The provision of healthcare is <NHS BOARD>'s public task as enabled under the National Health Service (Scotland) Act 1978 and is beyond the scope of this DPIA.

In certain circumstances it may be necessary to disclose limited information to the Police Service of Scotland or other agencies without the consent/knowledge of the service user. Guidance from General Medical Council is available to assist with type of disclosure.

Forensic medical information/samples will be collected with the cooperation of the data subject through a number of forensic medical examination procedures specific to the presentation of the service user.

Information/samples will be stored in accordance with <NHS BOARD>'s policies and procedures for forensic medical examinations which are attached as appendix I. These **must** be separate from the service user's health record in accordance with Records Management: NHS Code of Practice (SCOTLAND).

5. **What information is being provided to the people to whom the data relate to ensure that they are aware of this use of their personal data? – This is the 'right to be informed' (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/) and information such as privacy notices may be included as an attachment.**

How the NHS handles your personal health information (https://www.nhsinform.scot/care-support-and-rights/health-rights/confidentiality-and-data-protection/how-the-nhs-handles-your-personal-health-information)

<NHS BOARD>'s Data Protection Notice.
A specific privacy notice for law enforcement regarding rape and sexual assault.
Other public information leaflets (*see implementation guidance*)

6. **How will people's individual rights in relation to the use of their personal data be addressed by this process? (Rights are not applicable to all types of processing, and expert advice on this may be necessary.)**

<NHS BOARD> uses the following policies and procedures to ensure data subjects can exercise their rights.

Right of access:
See Appendix J
See Appendix K

Right to rectification:
See Appendix J

Right to object (where applicable):
See Appendix J

Right to restrict processing (where applicable):
See Appendix J

Right to data portability (where applicable):
Not applicable.

Right to erasure (where applicable):
Not applicable

Rights in relation to automated decision-making and profiling (where applicable):
Not applicable.

7. **For how long will the personal data be kept?- refer to our Document Storage Retention and Disposal Policy for advice**

<NHS BOARD> retains this information for ..... (*see implementation guidance*)

Who will have access to the personal data?

All Circumstances

<NHS BOARD> authorised personnel

Where the Police Service of Scotland are aware of the incident

The Police Service of Scotland's personnel

COPFS personnel

Depending on the services user's choices

Social Services personnel

Third sector personnel

Where the service user is a child or young person

Social Services personnel

8. **Will the personal data be routinely shared with any other service or organisation? – if yes, provide details of data sharing agreement(s) and any other relevant controls. Advice on data sharing requirements is in the Scottish Information Sharing Toolkit.**

Yes, there is an Information Sharing Agreement (ISA) in place between <NHS BOARD> and the Police Service of Scotland.

9. **Will the personal data be processed by a Processor e.g. an IT services provider? – [see Guidance Notes for the definition of Processor]. If yes, provide details of selection criteria, processing instructions and contract (may be attached separately).**

   Insert the details of any processors.

10. **Describe what *organisational* controls will be in place to support the process and protect the personal data (seek the advice of your Information Security Officer as necessary.)**

<NHS BOARD> has the following control measures in place.

Type of Control – examples	**Description**
Information Governance, Security and related policies	(*see implementation guidance*)
Staff training	(*see implementation guidance*)
Adverse event reporting and management	(*see implementation guidance*)
Physical access and authorisation controls	(*see implementation guidance*)
Environmental controls	(*see implementation guidance*)
Information asset management including management of backups and asset disposal	(*see implementation guidance*)
Business continuity	(*see implementation guidance*)
Information Asset Register	All information assets used are documented in the information asset register
Management of third parties and partners	(*see implementation guidance*)
Standard Operating Procedures	(*see implementation guidance*)

11. **Describe what *technical* controls will be in place to support the process and protect the personal data (seek the advice of your Information Security Officer as necessary).**

Type of Control – examples	**Description**
System access levels and user authentication controls	(*see implementation guidance*)
System auditing functionality and procedures	(*see implementation guidance*)
Operating system controls such as vulnerability scanning and anti-virus software	(*see implementation guidance*)
Network security such as firewalls and penetration testing	(*see implementation guidance*)
Encryption of special category personal data	(*see implementation guidance*)
Cyber Essentials compliance(if applicable)	(*see implementation guidance*)
System Security Policy (SSP) and Standard Operating Procedures(SOPs) (if applicable/ when available)	(*see implementation guidance*)
Details of ISO27001/02 accreditation (if applicable)	(*see implementation guidance*)
Add others where applicable	(*see implementation guidance*)

12. **Will personal data be transferred to outside the European Economic Area (EEA) or countries without an European Commission-designated adequate level of protection? – if yes, provide details of the safeguards that will be in place for the transfer(s).**

No (*see implementation guidance*)

13. Describe who has been consulted in relation to this process – e.g. subject matter experts, service providers, service users.

Subject matter experts

Service providers

<Insert consultations when done>

14. <u>In light of what is proposed, indicate what level of risk has been identified in relation to the following data protection principles:</u>

Principle	***Low/ Green***	***Medium/ Amber***	***High/ Red***
Personal data is processed in a fair, lawful and transparent manner	No Forensic Examination	Forensic Examination Forensic Examination – Third Party	
Personal data is collected for specific, explicit and legitimate purposes	No Forensic Examination	Forensic Examination	
Personal data is adequate, relevant and limited to what is necessary	No Forensic Examination	Forensic Examination	
Personal data is accurate, and kept up to date	No Forensic Examination	Forensic Examination	
Personal data is kept no longer than necessary	No Forensic Examination	Forensic Examination	
Personal data is processed in a manner that ensures adequate security	No Forensic Examination	Forensic Examination	

Note: Third party refers to any other person's information that may be captured by a forensic examination. E.g. The partner(s) of the service user, the alleged perpetrator of a crime or any other person who may have come into contact with the service user.

15. Risks and actions identified [see Guidance Notes for more information]. List all that you have identified and ensure that these integrate properly with our NHS Board's risk management process:

Description	Likelihood	Consequence	Overall Risk rating (LxC)	Mitigation/ Actions	Residual Risk	Risk Owner	Date
Loss of confidentiality of personal data protected by professional secrecy (Permanent loss of Forensic Medical Information (deletion, non recording, IT disaster)	Likely	Major	HR	<NHS BOARD> IT policies and procedures. Staff training. Documented forensic examination procedures.	Unlikely x Major = MR	NHS SIRO CG	
Inadmissibility of Forensic examination information as evidence	Likely	Major	HR	<NHS BOARD> Documented forensic examination procedures Staff training. Documented storage and transfer procedures.	Unlikely x Major =MR	NHS SIRO CG	
Transmission of data: Accidental disclosure via incorrect communications route	Likely	Major	HR	All <NHS BOARD> staff are trained in IG. All <NHS BOARD> staff are trained on the disclosure procedures. Standard operating	Unlikely x Major = MR	NHS SIRO CG	

				procedures with agreed communication methods and routes is in place.			
Inability to exercise rights(Service user)	Likely	Major	HR	See section 6	Unlikely x Major = MR	NHS SIRO CG	
Prevented from exercising control over their personal data (Third Party)	Almost Certain	Major	HR	Strict protocols mean that NHS will never try and identify an individual. It would be a reasonable expectation of the public that this information would be disclosed. On balance the rights of the service user and benefit to society of disclosure out weight the rights of third parties.	Unlikely x Major = MR	NHS SIRO CG	
Discrimination	Likely	Major	HR	NHS: Strict protocols are in place for the handling of health data to minimise the risk of inappropriate	Unlikely x Major = MR	NHS SIRO CG	

				disclosure,			
Reputational damage(Service user & Third Party)	Likely	Major	HR	NHS: Strict protocols are in place for the handling of health data to minimise the risk of inappropriate disclosure.	Unlikely x Major = MR	NHS SIRO CG	
Identity theft or fraud	Unlikely	Major	MR	NHS: Strict protocols are in place for the handling of health data to minimise the risk of inappropriate disclosure.	Remote x Major = MR	NHS SIRO CG	
Financial loss	Unlikely	Major	MR	NHS: Strict protocols are in place for the handling of health data to minimise the risk of inappropriate disclosure.	Remote x Major = MR	NHS SIRO CG	
Unauthorised reversal of pseudonymisation	Remote	Negligible	VLR	Pseudonymisation has not been specified	Remote x Negligible = VLR	NHS SIRO CG	

Risks that are associated with the general provision of Health and Social care and their related processes and systems by NHS BOARD are omitted as they are covered by other DPIA/PIA/Risk assessments.

16. Review and Sign-Off

Role	Advice/ Action/ Sign-Off	Date
IG/ Data Protection (DPO) Advice		
Information Security Officer Advice (questions 11 and 12)		
Others, if necessary e.g. Caldicott Guardian, Senior Information Risk Owner (SIRO)		
DPO opinion on whether residual risks need prior notification to the ICO		
Information Asset Owner(s) (IAO(s)) Sign Off		

17. Recommended Review Date:_____

Appendices

Appendix A: Standard Operation Procedure A – Transfer of information from an Agency / Service user to NHS.

Appendix B: Standard Operation Procedure B – Transfer of information from Service user and <NHS BOARD)

Appendix C: Standard Operating Procedure C – Transfer of information from <NHS BOARD> to the Police Service of Scotland

Appendix D: Standard Operating Procedure D – Transfer of information from <NHS BOARD> to a competent authority

Appendix E: Standard Operating Procedure E – Transfer of information from <NHS BOARD> by court order

Appendix F: Standard Operating Procedure F – Transfer of information from <NHS BOARD> to a competent authority

Appendix G: Standard Operating Procedure G – Transfer of information from <NHS BOARD> to another agency

Appendix H: Standard Operating Procedure H – Transfer of information from <NHS BOARD> to another agency

Appendix I: Standard Operating Procedure I – Forensic Medical Examination procedures

Appendix J: The <NHS BOARD>'s Data Protection Policy

Appendix K: The <NHS BOARD>'s Subject Access Procedure

Data Protection Impact Assessment Guidance

DPIA GUIDANCE NOTES

Question 2 - Special category personal data

The special categories of personal data are specified in Article 9 of the General Data Protection Regulation and include data about:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a person
- health
- sex life or sexual orientation

Personal data relating to criminal convictions and offences should be regarded as having the same special nature as those in the categories listed above.

Question 3 – Legal condition

It is illegal to process personal data without meeting adequately a legal condition.

For personal data which does not relate to any of the special categories (see definition above) the legal basis for the proposed processing must be one or more from the following list. Please note that 'data subject' means the person to whom the personal data relates.

- 6(1)(a) – Consent of the data subject
- 6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- 6(1)(c) – Processing is necessary for compliance with a legal obligation
- 6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person
- 6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- 6(1)(f) – Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject**.**

In NHS Scotland, in many cases condition 6(1)(e) will be the most relevant.

For personal data which relate to any of the special categories (see definition above) the legal basis for the proposed processing must be one or more from the following list:

- 9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
- 9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
- 9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- 9(2)(d) – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- 9(2)(e) – Processing relates to personal data manifestly made public by the data subject
- 9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- 9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
- 9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
- 9(2)(i) – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- 9(2)(j) – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

In NHS Scotland, in many cases condition 9(2)(h) will be the most relevant.

The Information Commissioner's Office (ICO) advises that public authorities will find using consent as a legal basis difficult. Therefore, if the proposed processing is to use consent as its legal basis you need to indicate why this is necessary and seek the advice of an appropriate IG professional.

Question 9 –Processor

Article 4 of the General Data Protection Regulation defines a Processor as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller. In practice, it includes organisations and companies

that provide services such as records storage, transport and destruction and IT services, where we ask them to carry out specific tasks using personal data on our behalf. IT suppliers, even if only accessing data/systems for support issues or bug fixes, are legally defined as a Processor. Processors may only be used to process personal information where they have provided sufficient guarantees to implement appropriate technical and organisational measures to comply with the law.

Question 15 – Risk Assessment

ASSESSING THE LEVEL (GRADE) OF THE RISK

1. Determine the **Likelihood (L)** of recurrence for the event using **Figure 1** (see below).

When determining the likelihood you should consider:

- The frequency of any previous occurrences e.g. how many times a data breach was reported due to this type of issue (e.g. lost records or records accessed without authorisation) in the last month? in the last year? in the last 5 years?
- You may need to check the Information Governance, Data Protection and Information Security incidents reported in your organisation in order to assess the likelihood.

Figure 1: Likelihood of Recurrence definitions

Descriptor	Remote	Unlikely	Possible	Likely	Almost Certain
Likelihood	Can't believe this event would happen – will only happen in exceptional circumstances (5-10 years)	Not expected to happen, but definite potential exists – unlikely to occur (2-5 years)	May occur occasionally, has happened before on occasions – reasonable chance of occurring (annually)	Strong possibility that this could occur – likely to occur (quarterly)	This is expected to occur frequently / in most circumstances – more likely to occur than not (daily / weekly / monthly)

2. Determine the **Consequence (C) rating** using **Figure 2 (see below)**

Look at **events** that **could lead** to the consequence, **not the consequence itself**

e.g. Examples of **Events:**

- records lost in transit (e.g. paper records sent by post)
- information recorded inaccurately or not recorded in the record
- data not available due to ransom-ware attack
- data lost due to error in IT systems – no useful backup available.
- confidential personal data sent by email to wrong addressee
- confidential personal data made available to external people due to poor role access definition and testing
- new system or changes in a system went life without appropriate change management (new or changes in data processing started without IG approval)

Examples of Consequence

- only 1 data subject affected but significant or extreme consequences
- e.g. missed vital treatment as a consequence of information not being issued to the Individual or health professional leading to death or major permanent incapacity or
- very sensitive data being exposed to people who don't need to know causes extreme distress (could be Individual or staff data)
- large amount of non-sensitive but personal identifiable data lost in the wind when in transit causing organisational embarrassment in the news for a week
- excessive health data shared with social worker (husband under domestic abuse investigation) causing direct threats and stalking.
- personal health data shared by a charity with private business for commercial/marketing purposes causing unwanted disturbance.
- reportable data breach to ICO causing monetary penalty.
- complaint from Individual to ICO results in undertaking for better access to health records.
- 1.6 million Individuals in Google Deepmind
- compliance Audit recommended
- Controller action required
- undertaking served
- advisory Visit recommended
- improvement Action Plan agreed
- enforcement Notice pursued
- criminal Investigation pursued
- civil Monetary Penalty pursued

Which consequence do you opt for?

NOT worst-case scenario and NOT most likely scenario

Opt for the “Reasonably foreseeable, worst case scenario” –

- If you got a phone call to tell you it had happened, you wouldn’t be surprised

Figure 2: Consequence Table

Descriptor	Negligible	Minor	Moderate	Major	Extreme
Objectives / Project	Barely noticeable reduction in scope / quality / schedule of an eHealth innovation (e.g. new system)	Minor reduction in scope / quality / schedule	Reduction in scope or quality, project objectives or schedule	Significant project over-run	Inability to meet project objectives, reputation of the organisation seriously damaged (e.g. Care.Data)
Injury (Physical and psychological) to patient / visitor / staff. e.g. issues with data quality, availability or confidentiality with physical or psychological consequence for the data subject.	Adverse event leading to minor injury not requiring first aid (e.g. data quality issues on instruction to patient re prescription)	Minor injury or illness, first aid treatment required	Agency reportable, e.g. Police (violent and aggressive acts) Significant injury requiring medical treatment and/or counselling. e.g. Staff member who attempted suicide, privacy compromised as A&E shared details beyond “need-to-know”.	Major injuries/long term incapacity or disability (loss of limb) requiring medical treatment and/or counselling.	Incident leading to death or major permanent incapacity (e.g. health records not released on time for making treatment decision causing death or major injury).
Patient Experience e.g. poor access to my records or difficulties to exert data protection rights.	Reduced quality of patient experience / clinical outcome not directly related to delivery of clinical care	Unsatisfactory patient experience / clinical outcome directly related to care provision – readily resolvable	Unsatisfactory patient experience / clinical outcome, short term effects – expect recovery <1wk	Unsatisfactory patient experience / clinical outcome, long term effects – expect recovery - >1wk	Unsatisfactory patient experience / clinical outcome, continued ongoing long term effects
Complaints / Claims e.g. Complaints due to data protection issues	Locally resolved verbal complaint	Justified written complaint peripheral to clinical care	Below excess claim. Justified complaint involving lack of appropriate care	Claim above excess level. Multiple justified complaints	Multiple claims or single major claim
Service / Business Interruption	Interruption in a service which does not impact on the delivery of	Short term disruption to service with minor impact on patient	Some disruption in service with unacceptable impact on patient	Sustained loss of service which has serious impact	Permanent loss of core service or facility

e.g. from constant small interruptions of ICT systems to big Business Continuity issues due to cyberattacks or core data centre being down beyond acceptable levels.	patient care or the ability to continue to provide service	care	care Temporary loss of ability to provide service	on delivery of patient care resulting in major contingency plans being invoked.	Disruption to facility leading to significant "knock on" effect
Staffing and Competence e.g. Poor data protection, confidentiality and ICT security training	Short term low staffing level temporarily reduces service quality (less than 1 day) Short term low staffing level (>1 day), where there is no disruption to patient care	Ongoing low staffing level reduces service quality Minor error due to ineffective training / implementation of training	Late delivery of key objective / service due to lack of staff. Moderate error due to ineffective training / implementation of training Ongoing problems with staffing levels	Uncertain delivery of key objective / service due to lack of staff. Major error due to ineffective training / implementation of training	Non-delivery of key objective / service due to lack of staff. Loss of key staff. Critical error due to ineffective training / implementation of training
Financial (including damage / loss / fraud) e.g. derived from compensation rights as per DPA, ICO or NIS fines, ransomware, etc.	Negligible organisational / personal financial loss (£<10k)	Minor organisational / personal financial loss (£10k-100k)	Significant organisational / personal financial loss (£100k-250k)	Major organisational / personal financial loss (£250 k-1m)	Severe organisational / personal financial loss (£>1m)
Inspection / Audit e.g. ICO or NIS interventions	Small number of recommendations which focus on minor quality improvement issues	Recommendations made which can be addressed by low level of management action.	Challenging recommendations that can be addressed with appropriate action plan.	Enforcement action. Low rating Critical report.	Prosecution. Zero rating Severely critical report.
Adverse Publicity / Reputation e.g. media attentions due to data breaches or cybersecurity attacks	Rumours, no media coverage Little effect on staff morale	Local media coverage – short term. Some public embarrassment. Minor effect on staff morale / public attitudes.	Local media – long-term adverse publicity. Significant effect on staff morale and public perception of the organisation	National media / adverse publicity, less than 3 days. Public confidence in the organisation undermined Use of services affected	National / International media / adverse publicity, more than 3 days. MSP / MP concern (Questions in Parliament). Court Enforcement Public Enquiry

Based on: Australian/New Zealand Standard: Risk Management (AS/NZS4360:2004) Risk Management Standard), (2004) Standards Australia/Standards New Zealand

Clinical Governance and Risk Management Standards (2005), NHS Quality Improvement Scotland

3. Use the risk matrix shown in **Figure 3** below to determine the risk grading for the risk. **L x C =R**

Figure 3: Risk Assessment Matrix

Likelihood	**Consequence**				
	Negligible	**Minor**	**Moderate**	**Major**	**Extreme**
Almost certain	LR	MR	HR	HR	HR
Likely	LR	MR	MR	HR	HR
Possible	VLR	LR	MR	MR	HR
Unlikely	VLR	LR	LR	MR	MR
Remote	VLR	VLR	VLR	LR	LR

In terms of grading risks, the following grades have been assigned within the matrix.

- Very Low Risk (VLR)
- Low Risk (LR)
- Moderate Risk (MR)
- High Risk (HR)

INFORMATION SHARING AGREEMENT

Victims of Rape and Sexual Assault

This Information Sharing Agreement sets out the arrangements for the sharing of information between NHS [insert board] and the Police Service of Scotland to support the service provision for victims of rape, sexual assault and sexual abuse.

[RELEVANT DATE]

Contents

Introduction

This Information Sharing Agreement (ISA) has been prepared to support appropriate sharing of information between NHS [insert board] and the Police Service of Scotland. (Hereafter referred to as the “parties”). A Data Protection Impact Assessment (DPIA) has also been developed and should be read prior to this for clarity on the process. The Police Service of Scotland will become the controller for the samples, copy health records and professional clinical statement when handed over to them, and will determine when this information can be shared and with whom. A data sharing agreement is currently in place within NHS [Insert Board] for sharing information with social work.

The aim of this document is to facilitate consistent, person-centred, trauma informed healthcare and forensic medical services with access to relevant services for anyone who has experienced rape, sexual assault or sexual abuse in Scotland. In addition, the ISA will encourage integrated working with agencies to improve outcomes for patients, service users, carers and their families.

Scottish NHS Boards will also need to work in partnership with local authorities, social care, education, the voluntary sector and other key agencies to ensure that services meet the needs of individuals who have been raped, sexually assaulted or experienced sexual abuse, to improve quality care and outcomes for that individual regardless of age or gender.

This document sets out the rules to be applied by the Health Board when sharing information with the other agencies noted in this agreement.

1 Parties, Scope and Purpose

1.1 Name and details of the parties who agree to share information

Trading name of parties subject to the ISA and Head Office address	Short name of the party	Role in this agreement : Controller or Processor (*)	ICO Registration
NHS [Insert Board] [Insert Address]	The Board	Controller	[Insert]
The Police Service of Scotland [Insert Address]	The Police	Controller	[Insert]

The aim of this ISA is to:
Facilitate the sharing of information between parties. When information has been shared from the NHS to the Police Service of Scotland, the Police Service of Scotland will then be the controller for that instance of the information.
Put in place a framework which will allow this information to be processed by the parties and exchanged in ways, which respect the rights and freedoms of individuals and in compliance with the law. Those individuals may include third parties for example current partner, family members, alleged perpetrator, and/or any relevant associates to support the prevention or detection of crime or the apprehension or prosecution of offenders.

1.2 Business and legislative drivers for sharing data

In March 2017, Her Majesty's Inspectorate of Constabulary in Scotland (HMICS) published a report that provided a strategic overview of forensic medical and healthcare services for victims of sexual crime. The report identified significant gaps and variation in the quality of services and made a number of recommendations to improve this. The report, the Chief Medical Officer for Scotland (CMO) was asked by the Cabinet Secretary for Health and Sport and the Cabinet Secretary for Justice, to chair a Taskforce to provide national leadership and oversight to help improve service provision in this area.
This Information Sharing Agreement template and supporting documentation has been developed by the Taskforce with the aim of facilitating the sharing of information between agencies responsible for the welfare of individuals who have been victims of sexual crime is increasingly important to improve safe and effective service provision and outcomes for victims. Proportionate and necessary information sharing is essential to the operation of a comprehensive system which has patients at its centre, allowing a level of consistency across Scotland.

1.2.1 Purpose(s) of the information sharing

Indicate how the controllers will decide upon changes in the purpose(s) of the information sharing	Jointly or independently
	Jointly

For the duration of the short life Information Governance Delivery Group, the Chief Medical Officer Taskforce will facilitate management of the information governance documentation which supports this agreement. Appropriate Information Governance experts from all agencies will be called upon to contribute to changes as and when necessary.

1.2.2 Legal basis for the processing and constraints

Without detriment of any other legal basis that may be applicable (e.g. criminal investigation, etc.) the following are the core legal basis for each of the parties to process the data in this agreement:

Data Protection Principles

The Parties have entered this Agreement to assist them with processing personal data in accordance with the data processing principles. Those principles are, in summary:

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner
(b) collected for specified, explicit and legitimate purposes
(c) adequate, relevant and limited to what is necessary
(d) accurate and, where necessary, kept up to date
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
(f) processed in a manner that ensures appropriate security of the personal data,

Accountability is central to General Data Protection Regulation: controllers are responsible for compliance with the principles and must be able to demonstrate this to data subjects and the regulator.

Constraints to Processing

As well as having to adhere to Data Protection principles, NHS Scotland also needs to take into consideration Caldicott Principles and the common law duty of confidentiality which can constrain what information can be shared and with whom. The personal data is shared with the Police Service of Scotland for the purposes of the prevention and detection of crime or the apprehension or prosecution of offenders, which in most cases will override the constraints to processing.

Caldicott Principles

The Parties acknowledge that the Caldicott Principles must be applied to the processing of personal data to ensure that the information is only shared for justified purposes.

Principle 1 - Justify the purpose(s) for using confidential information
Principle 2 - Only use it when absolutely necessary
Principle 3 - Use the minimum that is required
Principle 4 - Access should be on a strict need-to-know basis
Principle 5 - Everyone must understand his or her responsibilities
Principle 6 - Understand and comply with the law
Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

Common Law Duty of Confidentiality

The Parties also acknowledge that they owe a duty of confidentiality to all individuals. The General Medical Council's describes the duty of confidentiality in the following terms:

> "Information acquired by doctors in their professional capacity will generally be confidential under the common law. This duty is derived from a series of court judgments, which have established the principle that information given or obtained in confidence, should not be used or disclosed further except in certain circumstances. This means a doctor must not disclose confidential information, unless there is a legal basis for doing so."

It is generally accepted that the common law allows disclosure of confidential information if:

a) the patient consents
b) it is required by law, or in response to a court order
c) it is justified in the public interest.

The common law cannot be considered in isolation. Even if a disclosure of confidential information is permitted under the common law, the disclosure must still satisfy the requirements of GDPR/Data Protection Act 2018.

Legal basis	Party
General Data Protection Regulation **6(1)(e)** processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; **6 (1)(c)** processing is necessary for compliance with a legal obligation to which the controller is subject; (court order) **6 (1)(d**) processing is necessary in order to protect the vital interests of the data subject or of another natural person. **9 (2)(c)** processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; **9 (2)(g)** processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; **Preventing or detecting unlawful acts** **Data Protection Act 2018, Schedule 1, Part 2, 10** (1)This condition is met if the processing— (a)is necessary for the purposes of the prevention or detection of an unlawful act, (b)must be carried out without the consent of the data subject so as not to prejudice those purposes, and (c) is necessary for reasons of substantial public interest. (2) if the processing consists of the disclosure of personal data to a competent authority, or is carried out in preparation for such disclosure, the condition in sub-paragraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule). (3)In this paragraph— “act” includes a failure to act; “competent authority” has the same meaning as in Part 3 of this Act (see section 30).	NHS Board

Crime and taxation: general **Data Protection Act 2018, Schedule 2 (2)** (1)The listed GDPR provisions and Article 34(1) and (4) of the GDPR (communication of personal data breach to the data subject) do not apply to personal data processed for any of the following purposes— (a)the prevention or detection of crime, (b)the apprehension or prosecution of offenders, or (c)the assessment or collection of a tax or duty or an imposition of a similar nature, to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) to (c). (2)Sub-paragraph (3) applies where— (a)personal data is processed by a person ("Controller 1") for any of the purposes mentioned in sub-paragraph (1)(a) to (c), and (b)another person ("Controller 2") obtains the data from Controller 1 for the purpose of discharging statutory functions and processes it for the purpose of discharging statutory functions. (3)Controller 2 is exempt from the obligations in the following provisions of the GDPR— (a)Article 13(1) to (3) (personal data collected from data subject: information to be provided), (b)Article 14(1) to (4) (personal data collected other than from data subject: information to be provided), (c)Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers), and (d)Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in paragraphs (a)to (c), to the same extent that Controller 1 is exempt from those obligations by virtue of sub-paragraph (1). **The Data Protection Act 2018** **35(2)(b)** the processing is necessary for the performance of a task carried out for that purpose by a competent authority**.** **35(5)** The second case is where— (a) the processing is strictly necessary for the law enforcement purpose,	The Police Service of Scotland

(b) the processing meets at least one of the conditions in Schedule 8, and (c) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42). **Statutory etc purposes** **Data Protection Act 2018, Schedule 8 (1)** This condition is met if the processing— (a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and (b) is necessary for reasons of substantial public interest. **Administration of justice** **Data Protection Act 2018, Schedule 8 (2)** This condition is met if the processing is necessary for the administration of justice. **Protecting individual's vital interests** **Data Protection Act 2018, Schedule 8 (3)** This condition is met if the processing is necessary to protect the vital interests of the data subject or of another individual. **Safeguarding of children and individuals at risk** **Data Protection Act 2018, Schedule 8 (4)** **(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. **Legal Claims** **Data Protection Act 2018, Schedule 8 (6)** This condition is met if the processing— (a) is necessary for the purpose of, or in connection with, any legal proceedings(including prospective legal proceedings), (b) is necessary for the purpose of obtaining legal advice, or (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights. **DPA 2018 Sched 2, Pt 1, Para 2**, the Police Service of Scotland Form 052-003A will be submitted by Officers requesting submissions via these Legal Gateways where 'vital interests' are concerned and where non-disclosure "would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders." This would be required where consent was not given or could not be obtained. This may be where the victim is deceased or otherwise incapable of giving consent.	

In cases where consent is provided and police require to seize certain items whether it be samples, medical records etc. then the Police Service of Scotland could utilise a Force Form along the lines of the current Police Service of Scotland's Form 052-007 entitled Authorisation for the Recovery of Sensitive Records. This is currently used to seize specific records from victims in regard their particular investigation and is intended to stop Police taking possession of wholesale records. The form would stipulate what particular item Police wished to seize and a signed copy left with the relevant health authority.	

2 Description of the information to be shared

Data category	Controller(s)	PD*
Data items and categories will be listed in the Data Protection Impact Assessment for consistency.	NHS	PD

(*) PD – refers to Personal Data in the sense given within the EU General Data Protection Regulation (GDPR) and the Data Protection (UK, 2018) Act.

3 Description and manner of information sharing

3.1 Data flows

Data flows are detailed by data category in the Data Protection Impact Assessment for this agreement for the purposes of version control.

3.2 How data/information is to be accessed, processed and used

Processing (descriptor)	Associated standard operating procedure, policy or procedure (listed in Appendix 1) If applicable
The data to be processed is described in the Data Protection Impact Assessment for this agreement.	.

3.3 Summary of how decisions are going to be made with regards to the manner of the processing.

The manner of processing is detailed within the clinical guidelines for Clinical Pathways and Guidance for Healthcare Professionals Working to Support Adults who Present Having Experienced Rape or Sexual Assault in Scotland, and Clinical Pathway for Children and Young People who have Disclosed Sexual Abuse.

4 Impact assessments and preparatory work

The CMO Taskforce Information Governance Delivery Group developed Data Protection Impact Assessment supports this Information Sharing Agreement.

Mandatory statement: The parties acknowledge that any actions and countermeasures agreed as part of the Data Protection Impact Assessment reviews must be implemented by the responsible party. Deadlines and follow up to progress on those actions will be established as part of the DPIA review process.

5 Privacy information (transparency requirement)

A tiered approach to transparency will be followed in line with current guidance from the Information Commissioner's Office. All parties have a Data Protection Notice displayed on their website.

https://www.nhslanarkshire.scot.nhs.uk/data-protection-notice/

https://www.scotland.police.uk/access-to-information/data-protection/privacy-notices

The parties agree that further privacy notices may be produced as required for particular methods of processing in order to ensure appropriate transparency with the data subjects. The parties will take the advice of their DPO or DPOs in this regard.

Information will also be available from NHS Inform.

6 Accuracy of the information

As outlined in section 1.2.2, all parties are responsible for ensuring information, including personal data, is complete, accurate, relevant, accessible and timely.

The parties will ensure all staff using information shared by another party understand the limitations of such extracts and take all reasonable steps to confirm the accuracy of the information. This will involve confirming the accuracy of the information with the patient where possible.

It is the responsibility of all parties to ensure that their staff know how to respond to the identification of an actual or possible inaccuracy in information. The response to an inaccuracy should be managed according to a policy with procedures based on professional guidance.

It is the responsibility of the party identifying the inaccuracy to ensure that the controller of the record from which the information originated is informed about the inaccuracy.

As controllers, all parties have the responsibility for managing records, rectifying inaccuracies, and communicating updates with all other relevant parties.

7 Data retention and secure disposal

Data must be retained in accordance with the Scottish Government Records Management NHS Code of Practice (Scotland) which states Forensic Medical Records should be retained for 30 years.
Data which is no longer required must be disposed of in accordance with the Scottish Government Records Management NHS Code of Practice (Scotland) the NHS Scotland Information Security Policy Framework and each partner's policies and procedures.
The Police Service of Scotland follow their Record Retention Standard Operating Procedure (SOP) and Secure Destruction and Disposal of Data SOP.

8 The rights of individuals

Details of individual's rights are available in the Data Protection Impact Assessment and Data Protection Notice for the purpose of version control.

9 Security, risk and impact of the processing [each board is responsible for sections 9-13] Sections 9-13 will be completed by each Health Board as part of their formal risk assessment process. Whilst the aim is to align the process for victims across Scotland, each board may have different systems and policies in place. Therefore, local completion is essential.

[X] All relevant Security Policies applicable to the parties and systems used in this proposal are available and listed in Appendix 1.

[X] A qualified Information Security Officer has reviewed the adequacy of the attached Security Policies and has advised on the technical and organisational security risk level.

[X] A suitable process to document and monitor the security risk described in the Information Security and Governance Policies listed in Appendix 1.

[X] A Data Protection Impact Assessment has been produced and is available as listed in Appendix 1. Collaborative

[X] A competent, independent and free of conflicts of interests Data Protection Officer has been designated to inform the Controllers on the adequacy of this agreement and the corresponding compliance and any residual risks documented in the Data Protection Impact Assessment.

The security measures put in place across the parties ensure that:

[X] Wherever special categories of data are processed, the data will be encrypted at rest and in transit.

[X] Wherever special categories of data are transmitted over the internet, encryption protocols, such as Transport Layer Security (TLS) will be applied. Exceptions will be documented in the DPIA and any residual risk will require approval by the Senior Information Risk Owner (SIRO) of each organisation prior to processing such data.

[X] Only authorised individuals can access, alter, disclose or destroy data. This is achieved through work instructions, policies and procedures.

[X] Authorised individuals act only within the scope of their authority. This is achieved through the following work instructions, policies and procedures.

[X] If personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned. This is achieved through the following work instructions, policies and procedures (also listed in Appendix 1):

The security controls for the transmission of data applicable by each organisation will be:	X	Jointly agreed between the parties
		Independently decided by each party

The security controls applicable to locally held data by each organisation will be:		Jointly agreed between the parties
	X	Independently decided by each party

9.1 Agreed standards, codes of conduct and certifications

-

10 International transfers of personal data

Personal data shared in line with this agreement will be transferred to:

	EEA countries only
	Out with EEA
X	Will not be transferred outside the UK

10.1 List of countries where the data will be transferred to (if applicable).

N/A

11 Implementation of the information sharing agreement

11.1 Dates when information sharing commences

January 2020

11.2 Training and communications

All parties will have a Data Privacy Notice which will be provided to the data subject at the first point of contact. Third party data subjects will not be provided a data privacy notice in line with Schedule 2 (1)(2) of the Data Protection Act 2018.
The Police Service of Scotland will disseminate the content of this ISA by way of Force Memorandum and details will also be distributed via the Police Service of Scotland's Intranet. A copy of the final ISA between the NHS and the Police Service of Scotland will be held within the Policy Until.

11.3 There will be no requirement to conduct formal training of staff. Information sharing instructions and security controls

All relevant information sharing instructions, including but not exclusively any work instructions, policies or procedures, are listed in Appendix 1 and accepted by all parties.
Security is discussed at Section 9. PS employ the Government Security Classification (GSC) system of protective marking on all media types.

11.4 Non-routine information sharing and exceptional circumstances

NHS [insert board] will review requests to share information on a case by case basis, taking advice from the DPO, Senior Management, SIRO, and Caldicott Guardian.
The sharing of 'non routine' information in 'exceptional circumstances' will be assessed on a case by case basis taking into account the requirements of the prevention and detection of crime or the apprehension and prosecution of offenders where consent has not been obtained. The route taken will depend on whether consent has been obtained or not. This may lead to production of a warrant from COPFS or DPA Form (052-003A).

11.5 Monitoring, review and continuous improvement

NHS [insert board] holds an Information Sharing Agreement Register which is monitored and amended by the Data Protection Officer at regular intervals and tabled at the Information Governance Committee. ISA's will be amended in line with changes of legislation and reviewed at least yearly. A review can be triggered by any parties by contacting the CMO Taskforce who will convene a meeting of the Information Governance Reference Group to consider appropriate changes.
Any amendments should be taken to the Information Governance Forum for Scotland by the relevant DPO in order that the change can be escalated through the appropriate governance route above.

12 Sign-off

"We the undersigned agree to the details recorded in this Information Sharing Agreement; are satisfied that our representatives have carried out the preparatory work set out in the Information Sharing Tool-kit for Scotland and are committed to the ongoing monitoring and review of the scope, purpose and manner of the information sharing."

Name of the Party		
Authorised signatory	Title and name	
	Role	
Signature and date		
Data Protection Officer		
Senior Information Risk Owner		

Name of the Party		
Authorised signatory	Title and name	
	Role	
Signature and date		
Data Protection Officer		
Senior Information Risk Owner		

*Additional paragraph for **large numbers of parties delegating powers to a single signatory***
[DELETE THIS HEADING FROM FINAL VERSION BUT KEEP THE PARAGRAPH BELOW IF NEEDED]

The signatory has delegated sign off powers on behalf of:

- [party name]

Parties are required to sign off individually using the Multi Party Sign Off Form included in the toolkit.

13 Appendix 1: List of Work instructions, policies and procedures

Work instructions title	Organisation	Where to find this document (e.g. hyperlink)

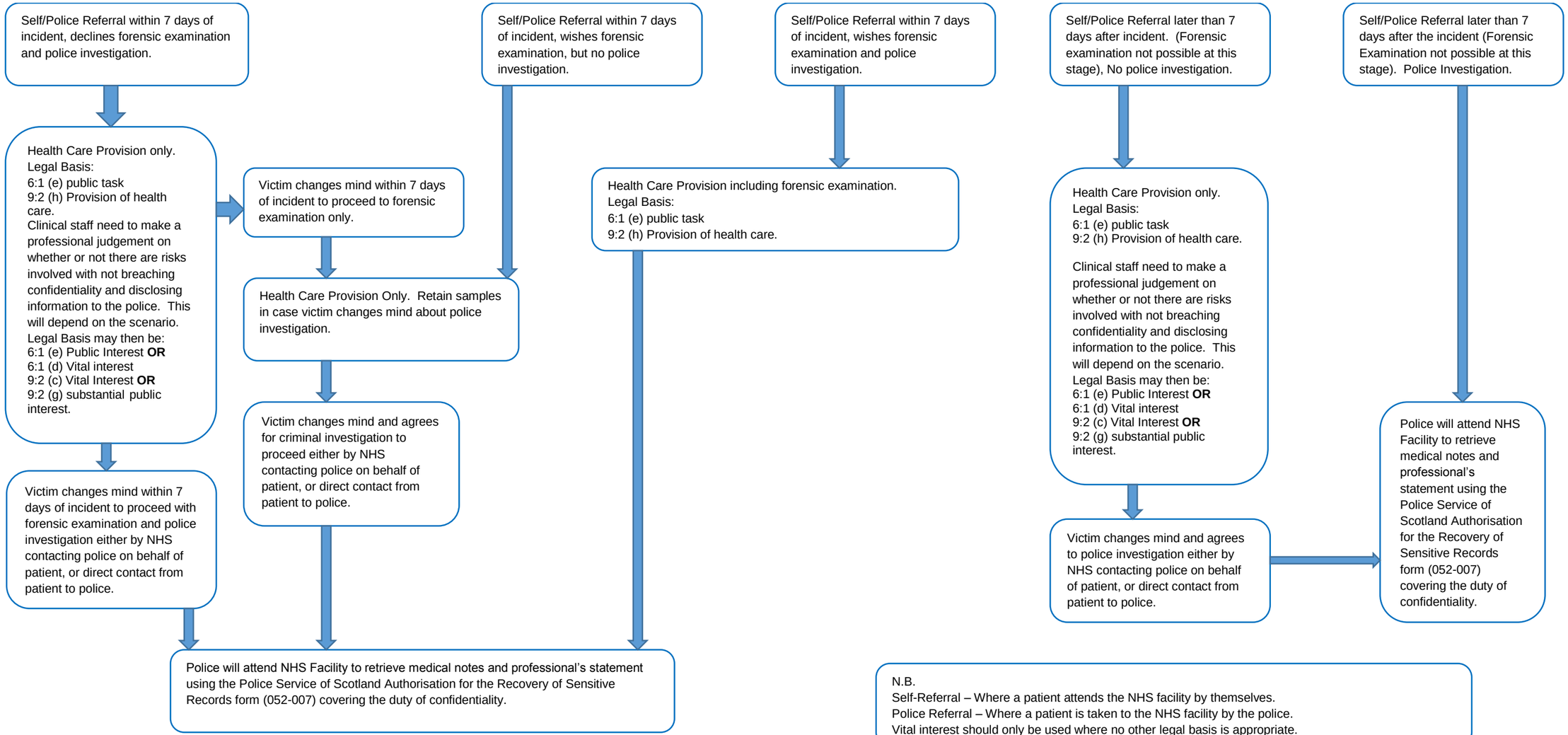
The above table should list all:

- Instructions for reaching agreement on any changes to the purpose of the sharing.
- All applicable and relevant Information Security and Governance Policies
- All Data Protection Impact assessments

14 Appendix 2: Data items and adequacy

Data Item	Source	Recipients	Data minimisation justification	For data linkage only

The above table should contain:
The list of all relevant data items/fields, which it has been agreed, can be shared under this ISA, indicating the source and the recipients, and any relevant supporting statement for information that may raise questions on data minimisation.



N.B.
Self-Referral – Where a patient attends the NHS facility by themselves.
Police Referral – Where a patient is taken to the NHS facility by the police.
Vital interest should only be used where no other legal basis is appropriate.

Consultation Questions :

1. **Do you have any general comments about the Data Protection Impact Assessment and Information Sharing Agreement?**

Data Protection Impact Assessment Questionnaire (DPIA)

2. **How will the Data Protection Impact Assessment bring clarity and consistency to NHS Boards?**

   Please be as specific as you can and include any resources or references to evidence that we should consider.

3. **Do you have any comments or suggested amendments to the information flow diagrams (as detailed in question 1 of the DPIA)?**

4. **Do you have any comments or suggested amendments to the sections of what personal data will be used and the legal conditions (as detailed in questions 2 and 3 of the DPIA)?**

5. **Do you have any comments or suggested amendments on the collection, use, transfer and updating of data (as detailed in question 4 of the DPIA)?**

6. **Do you have any comments or suggested amendments to the right to be informed and individual rights in relation to the use of personal data (as detailed in questions 5 and 6 of the DPIA)?**

7. **Do you have any comments or suggested amendments to data retention, disposal and sharing arrangements (as detailed in questions 7 and 8 of the DPIA)?**

8. **Do you have any comments or suggested amendments to organisations' processes (as detailed in questions 9 to 13 of the DPIA)?**

9. **Do you have any comments or suggested amendments to the sections on risk (as detailed in questions 14 to 16 of the DPIA)?**

10. **What additional guidance would you need to implement this document?**

11. **Do you have any general comments which are not covered in previous sections?**

Information Sharing Agreement (ISA) for victims of rape and sexual assault

Introductory Questions:

12. **Will the national information sharing agreement bring clarity and consistency to NHS Boards?**
    Yes
    No
    Don't know

    Please explain your answer being as specific as you can and include any resources or reference to evidence that we should consider.

13. **Does the national information sharing agreement acknowledge and support the person at the centre of the process?**
    Yes
    No
    Don't know

    Please explain your answer being as specific as you can and include any resources or reference to evidence that we should consider.

Children and young people services:

14. **Will the national information sharing agreement be of benefit to children and young people who have experienced child sexual abuse?**
    Yes
    No
    Don't know

    Please be as specific as you can and include any resources or references to evidence that we should consider.

15. **Will the national information sharing agreement be of benefit to non-abusing family and carers of children and young people who have experienced child sexual abuse?**
    Yes
    No
    Don't know

    Please be as specific as you can and include any resources or references to evidence that we should consider.

16. **Are there benefits to your organisation in implementing this agreement for children and young people?**
    Yes
    No
    Don't know

    Please explain your answer being as specific as you can and include any resources or reference to evidence that we should consider.

17. **Are there challenges to your organisation in implementing this agreement for children and young people?**
    Yes
    No
    Don't know

    Please explain your answer being as specific as you can and include any resources or reference to evidence that we should consider.

Adult services

18. **Will the national information sharing agreement be of benefit to adults who have experienced rape or sexual assault?**
    Yes
    No
    Don't know

    Please be as specific as you can and include any resources or references to evidence that we should consider.

19. **Will the national information sharing agreement be of benefit to non-abusing family and carers of adults who have experienced rape, sexual assault or child sexual abuse?**
    Yes
    No
    Don't know

    Please be as specific as you can and include any resources or references to evidence that we should consider.

20. **Are there benefits to your organisation in implementing this agreement for adults?**
    Yes
    No
    Don't know

    Please explain your answer being as specific as you can and include any resources or reference to evidence that we should consider.

21. Are there challenges to your organisation in implementing this agreement for adults?
Yes
No
Don't know

Please explain your answer being as specific as you can and include any resources or reference to evidence that we should consider.

General Questions

22. Are there any key areas missing, or any general amendments you would suggest?

Please be as specific as you can and include any resources or references to evidence that we should consider.

23. Is there sufficient existing guidance on when healthcare information should be shared with the police in the wider public interest?
Yes
No
Don't know

Please explain your answer being as specific as you can and include any resources or reference to evidence that we should consider.

24. What additional guidance would you need to implement this document?

25. Do you have any general comments or additions on topics which are not covered in previous sections?

Consultation on a new Data Protection Impact Assessment (DPIA) and Information Sharing Agreement (ISA) for victims of rape and sexual assault

RESPONDENT INFORMATION FORM

Please Note this form **must** be completed and returned with your response.

To find out how we handle your personal data, please see our privacy policy: https://beta.gov.scot/privacy/

Are you responding as an individual or an organisation?

☐Individual

☐Organisation

Full name or organisation's name

Phone number

Address

Postcode

Email

The Scottish Government would like your permission to publish your consultation response. Please indicate your publishing preference:

Information for organisations:

The option 'Publish response only (without name)' is available for individual respondents only. If this option is selected, the organisation name will still be published.

If you choose the option 'Do not publish response', your organisation name may still be listed as having responded to the consultation in, for example, the analysis report.

☐ Publish response with name

☐ Publish response only (without name)

☐ Do not publish response

We will share your response internally with other Scottish Government policy teams who may be addressing the issues you discuss. They may wish to contact you again in the future, but we require your permission to do so. Are you content for Scottish Government to contact you again in relation to this consultation exercise?

☐ Yes

☐ No

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at
The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-83960-050-0 (web only)

Published by The Scottish Government, August 2019

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS618430 (08/19)