

Releasing Information to the Police Guideline

Approval date:	13 January 2026
Version number:	1.0
Author:	David Morgan, Head of Information Governance and Data Protection Officer
Review date:	13 January 2029
Security classification:	OFFICIAL – Green: unclassified information

If you would like this document in an alternative language or format, please contact Corporate Services on 01595 743069.

Document reference number: HRGUI008

NHS Shetland Document Development Coversheet*

Name of document	Releasing Information to the Police Guideline		
Document reference number	HRGUI008	New or Review?	New
Author	David Morgan, Head of Information Governance and Data Protection Officer		
Information Asset Owner	David Morgan, Head of Information Governance and Data Protection Officer		
Executive lead	Colin Marsland, Director of Finance and Senior Information Risk Owner		
Review date	13 January 2029		
Security classification	OFFICIAL – Green: unclassified information		

Proposed groups to present document to:			
IGD	Caldicott Guardian (CG)	IGG	A&E
HMG	CHSC OPS	Police Scotland	

Date	Version	Group	Reason	Outcome
16/01/24	0.1	IGD	PI	PRO
23/02/24	0.2	Medical Director / Caldicott Guardian	PI	MR
	0.2	Director of Acute	PO and C/S	MR
	0.2	CHSC Operational Group	PO and C/S	No Reply
09/04/24	0.4	IGG	C/S	PRO
11/07/24	0.4	Police Scotland (Lerwick)	C/S	PRO
07/01/26	0.6	A&E	PI	PRO
13/01/26	0.8	IGG	FA	A

Examples of reasons for presenting to the group	Examples of outcomes following meeting
<ul style="list-style-type: none"> Professional input required re: content (PI) 	<ul style="list-style-type: none"> Significant changes to content required – refer to Executive Lead for guidance (SC)
<ul style="list-style-type: none"> Professional opinion on content (PO) 	<ul style="list-style-type: none"> To amend content & re-submit to group (AC&R)
<ul style="list-style-type: none"> General comments/suggestions (C/S) 	<ul style="list-style-type: none"> For minor revisions (e.g. format/layout) – no need to re-submit to group (MR)

<ul style="list-style-type: none">• For information only (FIO)	<ul style="list-style-type: none">• Recommend proceeding to next stage (PRO)
<ul style="list-style-type: none">• For proofing/formatting (PF)	<ul style="list-style-type: none">• For upload to Intranet (INT)
<ul style="list-style-type: none">• Final Approval (FA)	<ul style="list-style-type: none">• Approved (A) or Not Approved, revisions required (NARR)

*** To be attached to the document under development/review and presented to the relevant group**

Please record details of any changes made to the document in the table below

Date	Changes made to document
05/01/2024	First draft created. Saved as v0.1
16/01/2024	Reviewed by IGD and minor changes made: typos, format and structure. Saved as v0.2
03/04/24	Changes made following comments by the Directors of Acute and Medical. Section 2 , Introduction: added emphasis regarding the need for appropriate written authorisation. Section 4 , General principles: added more context and hyperlinks to NHS Scotland and GMC guidance and sub-section 4.1 , Points to consider. Section 8 , Disclosure Principles: renamed and hyperlinks added to an interactive GMC case-study. Section 9.4 , Court Orders: added information on challenging a Court Order. Section 9.5 , Witness Statements: guidance added. Section 9.6 , Added section on Sudden Death. Section 10.2 , Custody: renamed and notes added. Section 10.4 : CCTV: added notes on resourcing and out of hours requests. Section 12 , Out of Hours: more guidance added and contact details updated. Saved as v0.3
04/04/2024	Correction of typos. Saved as v0.4
11/07/2024	Revisions made following feedback from Police colleagues. Section 5 . Added text on email authorisation and the location of paper and electronic versions of the Police request form. Section 6.1 Added a qualification to the example. Section 7.3 Changed 'domestic violence' to 'gender-based violence' and added a sentence on Police access to patients. Section 9.5 Added a sentence about informing the Police if there will be a delay (or refusal) to providing a witness statement. Section 9.6 Added this section on Sudden Death. Section 10.4 Reworded to take account of urgent /public interest circumstances. Section 10.5 Added section on HSE and RIDDOR. Appendix 1 . Added a copy of the Police Request Form. Appendix 2 . Added a Flowchart. Saved as v0.5
21/11/2025	Updated following comments from Chief Nurse (Acute & Specialist Services). Updated DPO details – saved as version 0.6
07/01/2026	Added A&E flowchart developed in collaboration with A&E Senior Charge Nurse. Saved as version 0.7
13/01/2026	Approved by IGG. Saved as version 1.0

Contents

1. Purpose	7
2. Introduction	7
3. Data Protection law	7
4. General principles	7
4.1. Points to consider when responding to any request.....	8
5. Urgency of requests.....	8
6. Road traffic accidents	9
6.1. Example.....	9
7. Missing persons.....	9
7.1. Example – a child in care.....	10
7.2. Example – an adult with dementia	10
7.3. Example – a concerned family	10
7.4. Example – a dangerous person	10
8. Disclosure principles	11
9. Other disclosures.....	11
9.1. Serious incidents.....	11
9.2. Children	11
9.3. Terrorism	12
9.4. Court Orders	12
9.5. Witness Statements	12
9.6. Sudden Death.....	12
10. Further examples.....	13
10.1. Requests that are too broad	13
10.2. Request for information about a person in custody	13
10.3. Request about a patient suspected of causing a road traffic accident.....	14
10.4. Request for broad access to CCTV	14
10.5. A patient detained under the Mental Health Act absconds from hospital.....	14
10.6. RIDDOR Reportable Incidents and the Health and Safety Executive (HSE)	14
11. Help and support	15
11.1. Office Hours.....	15
11.2. Out of Hours	15
12. Summary	16
Appendix 1 - Police Scotland Request for Disclosure of Personal Data from External Organisations	17

1. Purpose

This document provides guidance on how staff should respond when Police Scotland request information about a patient or a member of staff. It should be read in conjunction with the Patient Confidentiality Policy, NHS Shetland Privacy Notice and Information Governance Policy.

2. Introduction

The information NHS Shetland holds about a patient or staff member should not be released to anyone, including the Police, unless the patient or staff member gives **consent and/or** the person requesting the information can provide the **appropriate written authorisation**.

There are, however, situations where a decision to share information with the Police without the person's consent can be justified. In general terms, such sharing will be either:

- necessary to prevent harm to the individual (and/or others)
- required by law

This guidance describes some situations where the person's consent is **not** required for their information to be shared with the Police.

3. Data Protection law

Data protection legislation does not prevent you sharing personal data with law enforcement authorities (known under data protection law as "competent authorities") who are discharging their statutory law enforcement functions. The UK GDPR and the DPA 2018 allow for this type of data sharing where it is **necessary** and **proportionate**.

When sharing information with the Police, deciding what is necessary and proportionate sharing is a **professional judgement**, therefore staff should seek the support and guidance of the Data Protection Officer (DPO) or a member of the Information Governance Department (IGD) if they have any doubts or concerns about the appropriateness of a Police request.

4. General principles

Each request for information needs to be **judged on the individual circumstances**. If in doubt, staff should discuss any concerns with the Data Protection Officer or Silver Command Acute/Community before releasing information.

The [NHS Scotland Code of Practice on Protecting Patients Confidentiality](#) is based on the Common Law Duty of Confidentiality. In relation to healthcare, it refers to the legal obligation of professionals to protect the privacy and confidentiality of patient information. It is a fundamental principle that establishes trust between patients and healthcare providers.

Under this duty, healthcare professionals, including doctors, nurses, and other staff, are required to keep all patient information confidential and not disclose it to any unauthorised individuals or third parties. This includes any personal, sensitive, or medical information shared by the patient during the course of their treatment or consultation.

In all cases, staff must **decide whether the harm caused by disclosing information** (for example, from breaching the duty of confidentiality, damaging trust between clinicians and patients, or any material harm to the person arising from the disclosure) **is outweighed by the benefits**.

Generally speaking, this balancing exercise will only favour disclosure where the disclosure is **necessary** and **proportionate**, in order to:

- prevent serious harm to the patient or others
- assist in the detection/prevention of a serious crime

The General Medical Council (GMC) has produced helpful guidance about the [disclosure of patient information](#) in the wider public interest.

4.1. Points to consider when responding to any request

You should remember the following points in relation to any request for information from the Police (from [generic guidance](#) produced by NHS England):

- Ask the Police to provide further information, if required, to assist you in ensuring any disclosure you make is necessary and proportionate. For example, helping you identify the correct person from your organisation's records or sharing details of the incident they are investigating to help establish whether there is a public interest justification for disclosing personal or confidential patient information.
- Consider whether it is appropriate to seek explicit consent from the individual before disclosing information to the Police. For example, would seeking consent put the patient or another person at risk of serious harm? Would it undermine a Police investigation by providing information to a suspect?
- Only provide information that is necessary and relevant for the specific enquiry. For example, if the Police want inpatient dates, only provide inpatient dates once you are satisfied with the validity of the request.
- Document what was requested, by whom, what was given and obtain a signature from the requester. This can be documented in the health and care record (for example, by adding a copy of the **Request for disclosure of Personal Data** form (Appendix 1) to the patient notes) or a log/register of disclosures.
- There may be times when it is appropriate to challenge a request from the Police. You should not feel under pressure to provide personal or confidential patient information.
- **Never give the Police an original health and care record to take away.**
- Where time permits or you are not sure what to do, you should seek advice, for example, from a Caldicott Guardian, IG lead, medical defence organisation or DPO.

5. Urgency of requests

It is rare that the Police will require information 'immediately' (this would normally be to prevent **serious** harm or to prevent/detect a **serious** crime). In such circumstances, staff should seek the guidance/advice of a senior manager and, in all cases, make a formal note of the request along with the name, rank and ID number of the Police Officer making the request.

In all other circumstances, staff should expect/ask Police Scotland to request the information via a correctly completed **Request for disclosure of Personal Data** form (Appendix 1). This should be authorised by a senior officer (usually an Inspector or above, for example a Chief Inspector, Superintendent or Chief Superintendent).

There may be occasions when a 'wet signature' is not possible because the authorising senior officer is 'off island'. In such circumstances, an authorising email from the senior officer is an acceptable alternative.

In the event that a Police Officer does not have / is not familiar with the above form, paper copies are available from the Accident and Emergency Department. It can also be downloaded from the Information Governance [Subject Access Request \(SAR\)](#) page on the Intranet.

The Police request forms should be passed to the Information Governance team in the same manner as a Court Order (see Section 8.4) and a copy should be kept in the patient's notes.

6. Road traffic accidents

Under road traffic legislation, the Police have the authority to obtain the name and address of an individual suspected of certain traffic offences. The duty to disclose this information is limited to information that may assist the Police in the identification of the driver.

It is also acceptable for staff to disclose the seriousness of the injuries/prognosis, as this will help the Police deploy the correct resources to the incident.

The duty to disclose does not extend to releasing full details of the patient's injuries, or who was with them. Examples of road traffic offences where there is a duty to disclose are:

- Driving whilst under the influence of drugs/alcohol
- Causing a road traffic accident
- Failing to stop at the scene of an accident

6.1. Example

In response to a serious road traffic accident the Police attend the Emergency Department (ED) and ask if 'Freddie Smith' has been admitted.

It is acceptable to confirm that the person has been admitted and the severity of the injuries. It is unlikely to be appropriate to disclose any other details of the patient's medical history unless it is pertinent to their outcome or the mechanism of injury.

7. Missing persons

When the Police seek information about someone who has been reported as missing, the decision to disclose will depend upon the individual circumstances of the request.

Acceptable grounds for disclosure are:

- if the person provides consent for the information to be disclosed to the Police (for example, if the person reported missing is an inpatient)
- the disclosure is deemed to be in the person's **immediate** best interests (this only applies to people who lack capacity)
- the disclosure is deemed to be 'in the public interest' and the amount of information disclosed is **necessary** and **proportionate** to prevent serious harm to the person and/or others (the decision, and reason(s) for disclosure, should **always** be documented in the clinical record)
- where a court orders the disclosure

Here are some ‘real world’ examples of Police requests for information related to people who are reported as ‘missing’:

7.1. Example – a child in care

A child in care, who is known to be at risk of exploitation, has gone missing. The Police contact the Child and Adolescent Mental Health Service (CAMHS) and ask for the names of anyone the child has spoken about in their CAMHS sessions.

Incidents involving missing persons under the age of 18 are considered to be high risk, especially if there are existing safeguarding concerns. As such, **necessary** and **proportionate** information should be released to the Police to assist them in locating the missing child/young person.

The Information Commissioner has made it very clear that **data protection law is not a barrier to sharing data to protect a child from harm**. Please see: [Sharing data to safeguard children](#).

If a child / young person discloses that they are missing in an attempt to flee the perpetrator of abuse, both the Police and Duty Social Worker should be informed. This is to help ensure the perpetrator is not inadvertently made aware of the whereabouts of the child / young person.

7.2. Example – an adult with dementia

Mr Smith has dementia and has gone missing from his home. The Police arrive at the Emergency Department (ED) and would like to know if Mr Smith has attended in the past 24 hours.

In this situation it would be reasonable to confirm whether or not Mr Smith attended the ED because he could be at risk of harm.

7.3. Example – a concerned family

A woman has not returned home from a night out. The Police arrive at the ED and ask if she has attended because her family are concerned for her welfare.

If the person is an in-patient, she should be asked if she consents to the disclosure of her presence in the hospital. The individual’s right to privacy must be respected and, in some cases, the person may not want to be ‘found’ (e.g. they are escaping gender-based violence).

In some circumstances, Police Officers may need to speak directly with the patient.

If the person does not want family members to know where they are, it is appropriate to tell the police that they are in the hospital but do not want their family to know.

The police can inform the person’s family that they are safe, but should not disclose where they are.

7.4. Example – a dangerous person

The Police are trying to locate a person who is armed and considered dangerous because they have already attacked a member of the public. The Police contact the ED and ask for information to help them locate the person.

In this situation, disclosure of **relevant** and **proportionate** information about the person’s potential whereabouts, and any known patterns of behaviour, is **likely to be in the public interest** because the individual could cause harm to self and/or members of the public.

8. Disclosure principles

As noted in Section 4 above, each request for information needs to be **judged on the individual circumstances**. If in doubt, staff should **discuss any concerns** with the Data Protection Officer or the Silver Command Acute/Community **before** releasing information.

In all cases, staff must decide whether the harm caused by disclosing information is outweighed by the benefits.

Generally speaking, this balancing exercise will only favour disclosure where the disclosure is **necessary** and **proportionate**, in order to:

- prevent serious harm to the patient or others
- assist in the detection/prevention of a serious crime

The General Medical Council (GMC) has produced detailed **guidance** on the [disclosure of patient information](#) together with a [framework to aid decisions](#) about disclosing personal information.

Staff can check their understanding of their disclosure responsibilities using the GMC's [interactive case-study](#). In this scenario, two police officers come to a doctor's clinic and ask for a list of all the patients who attended the clinic the previous Monday.

9. Other disclosures

There are a wide range of circumstances in which the Police may seek information about a patient or member of NHS Shetland staff. Here are some of the most significant:

9.1. Serious incidents

Data about a patient can be released to aid with the prevention or detection of a crime.

In these situations, the Police should always explain what they are investigating and what information they require. Always refer such decisions regarding the release of patient information to Silver Command Acute/Community.

When information is released, this should always be noted in the patient's record and the release strictly limited to what is necessary (for example, the police should never require a patient's full medical record).

In most cases, the patient's consent to release information should be requested, but there are some circumstances where this may not be appropriate. If you are not sure seek the advice of a Silver Command Acute/Community / IG Department.

All serious assaults, including gunshot incidents and the use of 'weapons' should be reported to the Police.

9.2. Children

In circumstances where a parent or legal guardian refuses to allow information about their child to be disclosed to the Police, clinicians should ultimately act in the best interest of the child. If a child is known to be the subject of a Child Protection Plan, or if the incident warrants the initiation of Child Protection enquiries, information can be shared without the consent of the child / young person or their parent/carer.

The Information Commissioner has made it very clear that **data protection law is not a barrier to sharing data to protect a child from harm**. Please see: [Sharing data to safeguard children](#).

The appropriateness of the disclosure should be confirmed by a relevant clinician.

9.3. Terrorism

Under terrorism legislation, staff are obliged to report suspected terrorist activity to the Police. Where possible, the decision to report should be discussed with a line manager.

9.4. Court Orders

If presented with a Court Order, all the patient information covered by the Court Order should be released.

Where a court order is ambiguous or appears to require disclosure of too much data, it may be possible to query it with the Court. The decision to query a Court Order needs to be made at an appropriate level of seniority and be actioned as quickly as possible.

More detailed information about disclosing personal information to the Courts and Procurator Fiscal can be found in Section 7.2.5 of the [NHS Scotland Code of Practice on Protecting Patients Confidentiality](#).

All Court Orders should be sent to the IG Department (shet.dpo@nhs.scot) without delay.

9.5. Witness Statements

With the exception of investigations under the Terrorism Act 2000, Prevention of Terrorism Act 2005 and the Road Traffic Acts, there is [no legal requirement to give a witness statement](#) to the Police.

However, assisting the Police with their enquiries is considered a civic and professional obligation and staff should be aware that the Court has the power to order a person to attend court to give evidence.

If a member of staff decides **not** to provide a statement (or there will be a delay whilst they seek advice) let the Police know as soon as it is practical to do so.

Any patient information disclosed in a witness statement should be:

- factual
- the minimum necessary to assist the Police with their investigation
- in keeping with the Code of Practice on Protecting Patients Confidentiality and any professional code of practice or conduct that applies (e.g. [NMC](#), [GMC](#), [HPC](#)).

9.6. Sudden Death

Where a sudden and unexpected death occurs within health premises and a doctor is unable to issue a death certificate, the Police may be required to carry out an investigation on behalf of the Procurator Fiscal (for example, a patient succumbs to an unexpected stroke, heart attack or similar).

These enquiries are perfectly normal and are a legal requirement to establish a cause of death and allow a death certificate to be issued. The enquiry may involve police asking to note statements from attending staff and taking possession of localised documents as productions. If

a full copy of a patient's health record is needed this would normally be obtained via a records request to the IG Department.

In some very exceptional circumstances, a death may be treated as suspicious, and the Police may be required to treat the bed space, or wider area, as a crime scene irrespective of whether the original injuries occurred within the hospital (for example a patient admitted to hospital with, and succumbing to, stab wounds). In such circumstances the Nurse in Charge of the Hospital and/or Silver Command (Acute) should liaise with the Police to establish how long the space is likely to be unavailable and alert Silver Command (Acute) and Gold Command.

Again, the police may ask to note statements from staff and take possession of documentation and other items such as blankets or other contaminated items.

In all cases where the Police require documentation, every effort should be made to retain the original and provide them with a copy. The Police may ask for any copy to be certified as a true copy with an undertaking that the original can be made available for court purposes if needed.

Managers will be mindful of the impact such events may have on staff and arrange appropriate support.

10. Further examples

It would be impractical to try and capture all the circumstances in which Staff may be asked to share information with the Police. The following examples capture some of the more common scenarios and give guidance on how staff might be expected to respond.

10.1. Requests that are too broad

Police attend the Emergency Department (ED) and ask for information on all patients attending with a hand injury because they are looking for someone who has allegedly punched and broken a window.

In this situation, it would not be suitable to disclose patient details, because such a generic request may involve disclosing the details of patients who have no link to the incident.

If the police attended and asked about a specific patient in relation such an incident, it would be acceptable to release this information.

10.2. Request for information about a person in custody

A Police Officer attends the ED and asks about the medical history of a person they have in custody.

Note: In Shetland, primary medical / urgent care services for people in custody are provided by the ED during office hours and the on-call custody clinician out of hours. The clinician attending the custody suite does not have access to the person's medical record (with the exception of their Emergency Care Summary). Consequently, the medical information available from the custody clinician is limited (even if it would be appropriate for it to be shared with the Police).

If someone needs medical treatment in custody, the required **information should normally be released to the clinician providing custody care**, not to the Police Officer.

In situations like this, staff should ask if the person has given consent for the release of their information to the Police and, if not, why not. If consent is not given/evidenced, staff should

seek the support of a senior clinician. As always, the decision to release patient information, and details of the information released, must be documented in the patient's record.

10.3. Request about a patient suspected of causing a road traffic accident

Police attend the ED with dashcam images of a driver they suspect caused a road traffic accident and then fled the scene. They think the driver may be receiving hospital treatment for minor injuries.

In this situation, staff should identify the patient to the Police. It would not be appropriate to release medical information about the patient without the patient's consent. Releasing details to help the Police identify the driver (name and address) is authorised.

10.4. Request for broad access to CCTV

Police attend at night and ask to view the CCTV recording of the front of the ED to try to identify people involved in an incident.

Try and obtain an image of anyone within the investigation time frame who meets the description provided by the Police. Patients not within the scope of a Police investigation should not normally have their images released without the production of a Court Order. Rarely, there may be time-sensitive circumstances with a clear public interest / safety justification for allowing the Police to view a CCTV recording without a Court Order.

Note: NHS Shetland is not resourced to provide Police access to CCTV images outside of office hours. If the Police confirm that access to CCTV images is essential and required without delay, contact Silver Command Acute/Community.

10.5. A patient detained under the Mental Health Act absconds from hospital

In this situation, the Police should be alerted and informed that the patient is detained under the Mental Health Act and whether or not they are considered to be at risk of harming themselves/others. It is acceptable to provide basic medical information to assist the Police, along with details of the patient's home address and any relevant phone numbers. Next of kin details may also be shared with the Police to help them find the patient as soon as possible.

10.6. RIDDOR Reportable Incidents and the Health and Safety Executive (HSE)

They Police may be involved in the investigation of some RIDDOR reportable incidents, but it is the responsibility of the Head of Department to ensure the timely reporting of RIDDOR incidents to the Health and Safety Executive.

Reporting certain incidents is a legal requirement. These reports inform the enforcing authorities (HSE, local authorities) about deaths, injuries, occupational diseases and dangerous occurrences, so they can identify where and how risks arise, and whether they need investigated.

HSE Inspectors are issued with a warrant of appointment, which specifies, usually by reference to the appropriate Sections of the Health and Safety at Work etc., Act 1974, what powers they have been given.

More information about the powers available to an HSE Inspector are set out in Section 6.2 of the [HSE Inspector Visit Procedure](#) on the Intranet.

With reference to information NHS Shetland holds about patients and staff, HSE Inspectors have the power:

- To require the production of, and take copies of, books and documents which are relevant to the inspection or investigation
- To interview any person and take written statements from any person he/she believes may give information relevant to the examination or investigation and require them to sign a declaration that the answers given are true

Whenever an Inspector uses, or seeks to use, any of their powers they must produce their warrant if asked to do so. Staff should:

- Ask to see the warrant before providing confidential information.
- **Never give the HSE Inspector an original health and care record to take away**
- Document the information requested, the Inspector's contact details, what was given and obtain a signature from the Inspector. This can be recorded in the health and care record or a log/register of disclosures.

11. Help and support

There are a wide range of situations in which Staff may be asked to share information with the Police and there is no overarching law that governs the disclosure of confidential information.

The common law and other laws that require or permit the disclosure of confidential information, including patient information, interact in complex ways and it is not possible to decide whether a use or disclosure of patient information would be lawful by considering any aspect of the law in isolation.

If you are not sure what you should do, speak with your line manager. If your line manager isn't available, or specialist support is required, please contact one of the people detailed below:

11.1. Office Hours

Sam Collier-Sewell
Data Protection Officer (DPO)
Tel: 07766 070 222
Email: shet.dpo@nhs.scot

Kirsty Brightwell
Caldicott Guardian (CG)
Tel: 07500 127437
Email: kirsty.brightwell2@nhs.scot

Alistair Morgan
Deputy DPO
Tel: extension 3684
Email: shet.dpo@nhs.scot

Susan Laidlaw
Deputy CG
Tel: 07884 226082
Email: susan.laidlaw2@nhs.scot

11.2. Out of Hours

Urgent requests for the release of patient (or staff) information out of hours should be a relatively uncommon event in Shetland.

All such requests should be discussed with the Nurse in Charge of the Hospital and/or Silver Command Acute/Community.

If the relevant senior staff are unavailable, or the correct course of action remains unclear, the Police should be asked to obtain a Court Order for the information they need.

Staff must comply with a Court Order (see Section 9.4, above).

12. Summary

Each request for information needs to be **judged on the individual circumstances**. If in doubt, staff should discuss any concerns with the Data Protection Officer and/or Silver Command Acute/Community **before** releasing the information.

In all cases, staff must decide whether the harm caused by disclosing information (for example, from breaching the duty of confidentiality, damaging trust between clinicians and patients, or any material harm to the person arising from the disclosure) is outweighed by the benefits.

Generally speaking, this balancing exercise will only favour disclosure where the disclosure is **necessary** and **proportionate** to:

- prevent serious harm to the patient or others
- assist in the detection/prevention of a serious crime

Any decision to release patient information, and details of the information released, must be **documented in the patient record**.



Request for Disclosure of Personal Data from External Organisations

(Data Protection Act 2018 – Schedule 2, Part 1(2))

This form is used to request personal data from another organisation or company. Officers / staff requesting such data should familiarise themselves with the Data Protection Standard Operating Procedure (SOP) and Information Sharing SOP, **prior** to completion of this form.

Organisation Holding the Data	
Organisation	
Contact Name	
Position	
Address	
Telephone	
Email	

I am making enquiries on behalf of the Police Service of Scotland which are concerned with: (please tick all relevant boxes which apply)

- (a) Prevention and detection of crime
- (b) Apprehension and prosecution of offenders

In a case where:

- The personal data requested is needed for the purposes indicated above, and a failure to provide information will be likely to prejudice those matters.
- or:**
- The individual whose personal data is sought should not be informed of this request as to do so would prejudice the matters described above.

I confirm all relevant Police Scotland systems have been checked prior to the submission of this request and details of those checks are recorded in a Police Scotland notebook / daybook.

The Data Protection Act 2018, Schedule 2 Part 1 Paragraph 2 (Crime & taxation: general) applies where personal data is disclosed by an organisation subject to the GDPR, to the police, for the purposes of **the prevention or detection of crime or the apprehension or prosecution of offenders**. It restricts the application of the GDPR data protection principles and subject rights (as listed in the Data Protection Act 2018 at Schedule 2 Part 1 Paragraph 1) to the extent that the application of those provisions would be likely to prejudice **the prevention or detection of crime or the apprehension or prosecution of offenders**.

OFFICIAL

Data Requested – Data Subject	
Name	
Date of Birth	
Address	
Nature of Enquiry	

Data Requested and Reason for Request

I certify that the data is required for the reason(s) stated above. I understand that if any information on this form is omitted or wrong I may be committing an offence under Data Protection Act 2018, Part 6, Section 166

Requestor Details			
Name			
Rank			
Signature			
Date		Telephone	

Supervisor Countersignature (Inspector & above)			
Name			
Rank			
Signature			
Date		Telephone	

Completing / Sending / Giving the Form

The completed form should be sent / given to the organisation and one a copy retained by the requestor.

Please note that this form can **only** be sent by email if the Government Security Classification (GSC) rules for handling 'OFFICIAL' information are followed, i.e. the recipient's email address must be on a network server or domain that has been added to the Police Scotland email 'White List'. For more information on emailing this form, please refer to the Information Security SOP, or contact Information Management / Information Security.

OFFICIAL

Appendix 2 - Decision Making Flow Chart

