Policy Document

Reference: DSP17

Access to Personal Information (Subject Access Request - SAR)

Version:	**2.1**
Date Ratified:	**July 2022 by Executive Digital and Data Security & Protection Group**
To Be Reviewed Before:	**July 2025**
Policy Author:	**Data Security & Protection Manager**
Executive Lead:	**Medical Director/Caldicott Guardian**

Version Control Schedule

Final Version	Issue Date	Comments
1	June 2021	New Policy document, required to assist staff to meet their obligations under the Data Protection Act 2018 Approved by Data Security & Protection Group (06.04.21) Approved by Policy Review Group (May 2021) Ratified by Executive Data Security & Protection Group 08 June 2021
2	September 2021	Minor amends: Page 4 – further clarification of what constitutes a PDR request Page 5 – clarification on data contained within the ICR not being applicable to SARs made to UHNM Page 15 – addition of link to ICO guidance and clarification on technology limitations. Page 16 – addition of clarification regarding unstructured files
2.1	July 2022	Minor amends: Page 11 - inclusion of reference to flowchart to guide on inappropriate access investigation process Appendix 2 – Inappropriate access investigation flowchart Page 10 – inclusion of requirement for SAR specific training

Consultation

Version	Team	Date	Comments
2.1 (Draft 0.1)	Records Services Operational Group	May 2022	Previously received approval from H.R. re. the Inappropriate Access Flowchart. Taken to RSOG for formal approval

REFERENCES

Data Protection Act (2018)

General Data Protection Regulation (EU GDPR 2016/679)

DSP18 – Overarching Data Security & Protection Policy

G09 – Management, Protection & Disclosure of Employment Related Information Policy

DSP17(S1) - SAR Procedure

DSP17(S2) - Disclosures to Law Enforcement & Other Investigative Agencies SOP

Statement on Trust Policies

The latest version of 'Statement on Trust Policies' applies to this policy and can be accessed here

CONTENTS **Page**

1. INTRODUCTION

1.1 This policy details the requirements to be met when dealing with requests for access to personal information as laid down by the Data Protection Act 2018 and the General Data Protection Regulations 2016, in relation to living individuals, the Access to Health Records Act 1990, specifically in relation to requests for health records of deceased individuals, and also requests for access to medical reports as laid down by the Access to Medical Reports Act 1988.

1.2 The Trust will provide information to its staff and members of the public, in accordance with the legislation, via its procedures and practices. A definition of the different types of information is included in section 4 below.

Subject Access Request (SAR) – a request for personally identifying information made by a data subject, relating to health records or staff employment records – these requests are handled by either the Health Records Dept. or the Trust H.R. Dept.

Personal Data Request (PDR) - A request for personally identifying information which does not fall within the SAR definition above. Examples of a PDR would be a request for e-mails stored on the Trust Network which names the individual or administrative documents which would not fall within the health record for example, Theatre Lists. These requests are handled by the Data Security & Protection Team.

Privacy Information Request (PIR) - This is a request, generally received as the result of a complaint, where an allegation of inappropriate access to patient and/or staff records has taken place by Trust staff. These requests are handled by the Data Security & Protection Team.

Further Advice on any request for information can be sought from:

The Data Protection Officer (DPO)
The Data Security & Protection Team (DSP Team)
Caldicott Guardian (CG)

1.3 This policy also details other considerations that should be taken into account when dealing with such requests, including the requirements of the following legislation:

Children Act 2004
Crime and Disorder Act 1998
Mental Capacity Act 2005

1.3 It is important that all staff understand the requirements of these Acts, and the part that they have to play in ensuring that the Trust complies with these legal obligations, as well as other guidance issued by the Department of Health, Digital Health, the General Medical Council (GMC), the Information Commissioner's Office (ICO), as regulator of the Data Protection Act (DPA), other professional bodies and other advisory groups to the NHS. Such guidance includes (but is not limited to):

Confidentiality: NHS Code of Practice 2003
Records Management: NHS Code of Practice (Part 1: 2006 & Part 2: 2009)
BMA guidance – Access to health records by patients 2008
HSC 1999/001 - The Provision of Patient Information by NHS Trusts to the DSS 1999
ICO Guidance

1.4 It is important that all staff understand their responsibilities when handling requests for personal identifiable and special category information and that they are aware that failure to follow the guidance provided will result in disciplinary action, in accordance with Trust procedures. Advice and guidance on the procedures to follow when answering these requests can be found in the Subject Access Procedure (Ref: DSP17[S1]) and the Disclosures to Law Enforcement & Other Investigative Agencies SOP (Ref: DSP17[S2])

2. STATEMENT OF INTENT / SCOPE OF THE POLICY

2.1 This policy applies to the University Hospitals of North Midlands NHS Trust, referred to as the 'Trust', and includes all hospitals, units and community health services managed by the Trust.

2.2 The policy applies to all health records and all staff records as defined in Section 1.2 above, both manual & computerised, including joint records, for example health and social care records. The policy applies to all requests for such information whether originating from the data subject, solicitor, police, employee or anybody else.

2.3 Wherever, throughout the policy, the term 'record' is used this means both the manual file and the electronic record, including audio, visual and photographic information.

2.4 This policy applies to all those working in the Trust, in whatever capacity. A failure to follow the requirements of the policy may result in investigation and management action being taken as considered appropriate. This may include formal action in line with the Trust's disciplinary or capability procedures for Trust employees; and other action in relation to other workers, which may result in the termination of an assignment, placement, secondment or honorary arrangement. Non-compliance with the Policy and/or the Data Protection Act (2018) may also lead to criminal action being taken.

3. SUMMARY

This policy provides guidance on dealing with requests for access to personal information. This includes, regardless of which team is responsible for handling the request:

- Patient Health Records
- Staff Human Resources Records
- Occupational Health Records

Separate Procedure document (Subject Access Procedures) is also available on the Information Governance microsite.

4. DEFINITIONS

4.1 Data Subject

Data Subjects are the people to which the information relates. Within the workplace, they may be current employees, people applying for jobs or former employees. Data subjects might also be customers, suppliers, clients, patients, former patients, or other people information is held about.

4.2 Subject Access

Individuals whose information is held by the Trust have rights of access to it, regardless of the media that the information may be held/retained on. This is known as a subject access request.

4.3 Health Record

Data Protection legislation defines a health record as a record consisting of information about the physical or mental health or condition of an identifiable individual made by or on behalf of a health professional in connection with the care of that individual.

A health record can be recorded in computerised or manual form or in a mixture of both. It may include such things as; hand-written clinical notes, letters to and from other health professionals, laboratory reports, radiographs and other imaging records e.g. X-rays and not just X-ray reports, printouts from monitoring equipment, photographs, videos and tape-recordings of telephone conversations.

The Trust feeds data into the Staffordshire-wide Integrated Care Record (ICR) 'One Health & Care'. Data provided for any requests made to the Trust for health record information will only include information taken from Trust-owned systems and will not include data taken from the ICR.

4.4 Employee Record

The employee record should be taken to consist of all information held regarding an individual other than that which may relate to that individual as a patient of Trust.

An employee record can be in computerised or manual form or in a mixture of both. It may include such things as; hand-written management notes, training records, occupational health records, letters to and from the employee or other members of staff, photographs, videos and, tape-recordings of telephone conversations.

4.5 Subject Access Request (SAR)

A request for personally identifying information made by a data subject, relating to health records or staff employment records – these requests are handled by either the Health Records Dept. or the Trust H.R. Dept.

4.6 Personal Data Request (PDR)

A request for personally identifying information which does not fall within the SAR definition above. Examples of a PDR would be a request for e-mails stored on the Trust Network which names the individual. These requests are handled by the Data Security & Protection Team.

4.7 Privacy Information Request (PIR)

This is a request, generally received as the result of a complaint, where an allegation of inappropriate access to patient and/or staff records has taken place by Trust staff. These requests are handled by the Data Security & Protection Team.

4.8 Appropriate Health Professional

Under the Data Protection Act 2018 "Health Professional" means any of the following;

a) A registered medical practitioner
b) A registered dentist as defined by section 53(1) of the Dentists Act 1984,

c) A registered dispensing optician or a registered optometrist as defined by section 36(1) of the Opticians Act 1989,

d) A registered pharmacist or a registered pharmacy technician within the meaning of article 3(1) of the Pharmacy Order 2010 or a registered person as defined by Article 2(2) of the Pharmacy (Northern Ireland) Order 1976,

e) A registered nurse, midwife or health visitor,

f) A registered osteopath as defined by section 41 of the Osteopaths Act 1993

g) A registered chiropractor as defined by section 43 of the Chiropractors Act 1994,

h) A child psychotherapist

(i) A scientist employed by a health service body as head of a department.

(j) "social work professional" means any of the following—

(i) a person registered as a social worker in England in the register maintained under the Health and Social Work Professions Order 2001 (S.I. 2002/254);

(ii) a person registered as a social worker in the register maintained by Social Care Wales under section 80 of the Regulation and Inspection of Social Care (Wales) Act 2016 (anaw 2);

(iii) a person registered as a social worker in the register maintained by the Scottish Social Services Council under section 44 of the Regulation of Care (Scotland) Act 2001 (asp 8);

(iv) a person registered as a social worker in the register maintained by the Northern Ireland Social Care Council under section 3 of the Health and Personal Social Services Act (Northern Ireland) 2001 (c. 3 (N.I.)).

The '**appropriate health professional'** is defined as either;

1. *"The 'health professional' who is currently or was most recently responsible for the clinical care of the data subject in connection with the information which is the subject of the request."*

2. Or where there may be more than one such person, the 'appropriate health professional'' will be:

   "The 'health professional' who is the most suitable to advise on the matter to which the information/subject of the request relates"

3. Or in the absence of anyone else who might qualify for the above role, the 'appropriate health professional'' will be:

   "A 'health professional' who has the necessary experience and qualifications to advise on the matters to which the information/subject of the request relates"

4.9 Appropriate Manager

The **'appropriate manager'** would be a senior Human Resources Manager in relation to any staff records that are held centrally by the Human Resources Department or the employee's line manager (or in the case of staff employed on the Wards, the Ward Manager) in relation to the records which they themselves hold and are responsible for.

4.10 Third Party Information

Information **from** an individual who is not the subject of the record, e.g. a relative of a patient, or a colleague, which is included in the subject's record is 'third party information'. This would include employee references or information in a child's health record from the child's parents. Similarly, information **about** a relative is 'third party information', as is any information about colleagues.

Information from a health professional who has compiled, or contributed to, the health record or has been involved in the care of the patient in his capacity as a health professional would not usually be considered third party information and should be disclosed unless serious harm to that health professional's physical or mental health or condition is likely to be caused by giving access.

Similarly, information from a manager who has compiled, or contributed to, an employee record or has been involved in the management of that employee would not usually be considered third party information.

4.11 Serious Arrestable/Indictable Offences

The Serious Organised Crime and Police Act 2005 updated the structure of police powers. The concept of arrestable and serious arrestable offences under the Police and Criminal Evidence Act 1984, which is often relied upon as the main criteria in the exercise of many police powers, were replaced by the Serious Organised Crime and Police Act 2005 with the term "indictable offence".

In order to warrant the disclosure of information offences would usually be among the most serious crimes and would generally only be tried before a jury in the Crown Court. These crimes include murder, manslaughter, rape, kidnapping, grand theft, robbery, burglary, arson, conspiracy, fraud, and other major crimes, as well as attempts to commit them.

As a guide an offence which is serious / indictable may be an offence which causes:

a) *Serious harm to the state*
b) *Serious injury to any person*
c) *Serious interference*
d) *Death*
e) *Substantial financial gain*

f) Serious financial loss

Further advice should be sought from the Data Security & Protection (DSP) Team or the Ministries Team and Caldicott Guardian to determine whether the offence justifies disclosure.

5. ROLES AND RESPONSIBILITIES

The Trust Board is ultimately responsible for ensuring the Trust meets its legal responsibilities, and for the adoption of internal and external governance requirements. The Performance & Finance Committee will be updated on DSP issues via highlight report.

Chief Executive
The Chief Executive as the Accountable Officer for the Trust has overall accountability and responsibility for DSP throughout the Trust and is required to provide assurance that all risks to the Trust, including those relating to information, are effectively managed and mitigated.

Senior Information Risk Owner (SIRO)
The Trust SIRO is responsible to the Chief Executive for Data Security & Protection and acts as an advocate for information risk on the Trust Board.

Caldicott Guardian
The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of Personal Identifiable Data (PID). The Caldicott Guardian is responsible for ensuring PID is shared in an appropriate and secure manner.

Head of Data Security & Protection/Data Protection Officer
The Head of Data Security & Protection/Data Protection Officer (DPO) has overall responsibility for managing the data security & protection function and as DPO will advise and monitor compliance with the GDPR and DPA. They are responsible for ensuring effective management, accountability, compliance and assurance for all aspects of the data security & protection agenda. They will also be the first point of contact with the Supervisory Authority – the Information Commissioner's Office.

Head of Data Quality & Clinical Coding
Will work closely with the Data Security & Protection team to provide information quality assurances across all areas of Trust activity. Within this context, the Data Quality Group provides and receives regular reports to and from the Data Security & Protection Executive Group.

Information Asset Owners (IAO)
Designated Information Asset Owners (IAOs) are responsible for providing assurance to the SIRO that information risks, within their respective areas of responsibility, are identified and recorded and that controls are in place to mitigate those risks.

Information Asset Administrators (IAA)
Information Asset Owners can appoint Information Asset Administrators (IAAs) to support them in the delivery of their information risk management responsibilities. IAA ensure that policies and procedures are followed, recognise actual or potential security incidents and take steps to mitigate those risks, consult with their IAO on incident management and ensure that information asset registers are accurate and up to date. Where an IAA is not in place, this function is carried out wholly by the IAO.

Data Security & Protection Manager
The Trust's Data Security & Protection Manager is responsible for supporting the Data Protection Officer in the implementation of the Trust's DSP agenda.

Data Security & Protection Facilitator
The Trust's Data Security & Protection Facilitator(s) is responsible for supporting the Data Security & Protection Manager in the delivery of the DSP agenda.

Data Security & Protection Executive Group (DSPEG)
The SIRO and Caldicott Guardian are joint chair of the Trust's DSPEG. This group is responsible for receiving assurances relating to the day to day management of the individual components of the Trust's Data Security & Protection Framework.

Data Security & Protection Operational Group (DSPOG)
The Data Protection Officer chairs the Trust's DSPOG. This group is responsible for overseeing the day to day management of the individual components of the Trust's Data Security & Protection Framework.

The Data Security & Protection Governance pack provides more detail on the make-up of the Groups which provide assurance that the Trust meets its obligations around data security & protection.

Information Security Manager (RA and Privacy)
Provides advice to the Trust, ensuring compliance, and conformance, with local and national requirements, and, generally, on information risk analysis/management incorporating the Privacy Officer role which focuses on ensuring privacy related alerts from electronic systems (e.g. Summary Care Record) are investigated for appropriateness, as well as other privacy compliance work as necessary.

Cyber Security Lead
Provides advice to the Trust, ensuring compliance and conformance, with local and national requirements and, generally, on cyber security issues across the Trust

Health Records Manager
Oversees the operational management of the Trust's paper health records ensuring that security is maintained in accordance with the legislation. The Health Records function also provides the subject access function for patients to access their clinical records.

Assistant Director of Human Resources/Governance Lead
Has responsibility for ensuring that the HR function meets the legislated requirements of the Data Protection Act 2018 in terms of security of information and access to records by staff (both current and former).

All Staff
All staff, via job roles and contracts of employment/professional registrations must comply with specific data security related legal and ethical obligations, including the need to undertake mandatory Data Security & Protection training, and therefore must be aware of the related standards which impact within their area of responsibility. Staff involved in the processing of Subject Access Requests must undertake role specific training which concentrates on the specific areas of the Data Protection Act which covers patient access rights. Individual staff must ensure that they make themselves aware of all policies and associated Standard Operation Procedures referenced in this document and abide by their contents. Any personal and corporate information, is managed legally, securely, and efficiently in order to assist in the delivery of the best possible care/practice. Staff can email the Data Security & Protection team on DSPUHNM@uhnm.nhs.uk with any data security related queries.

6. THE POLICY

All requests for access to information made under the Data Protection Act 2018, must be logged on a central system i.e. Staff requests will be recorded in HR; Medical Records will record all requests for access to medical records.

6.1 Subject Access SOP

The Trust has drafted a formal document, the Subject Access Standard Operations Procedure, which goes into detail about the process of handling subject access requests. It provides information about who to contact for advice. Further guidance is available in the Data Security, Protection & Confidentiality Manual which is available on the Data Security & Protection Intranet page. The Subject Access SOP must be followed when handling all requests for information from subjects. Failure to adhere to the SOP may result in disciplinary action, according to the Trust HR policies. Further advice is available from the DSP team (dspuhnm@uhnm.nhs.uk)

6.2 Disclosures of Personal Identifying/special Category Information to Law Enforcement and other Investigative Agencies SOP (Law Enforcement Disclosures)

The Trust has drafted a formal document to advise staff, in detail, about the procedure for handling requests for information for the purposes of investigation, to advise when it is acceptable to disclose information. Further guidance is available in the Data Security, Protection & Confidentiality Manual which is available on the Data Security & Protection Intranet page. The Law Enforcement SOP must be followed when handling all requests for information from investigative agencies. Failure to adhere to the SOP may result in disciplinary action, according to the Trust HR policies. Further advice is available from the DSP team (dspuhnm@uhnm.nhs.uk)

7. REQUESTS FOR INFORMATION FROM THE POLICE

The Trust wishes to foster good relations with the police, and to play its part in keeping the public safe and protecting it from crime. However, the Trust also has a duty to protect the confidentiality of its patients and staff, whether they are in hospital or in the community, and whether they are alive or dead.

This duty is breached where information about a patient – **including the mere fact that she/he is a patient** – is disclosed to someone else including the police.

The Trust has a duty to comply with the provisions of the Data Protection Act 2018. It follows that information may only be disclosed with the consent of the data subject, save in exceptional circumstances.

Instructions on handling requests for information from the Police are contained in the Disclosures of Personal Identifying/special Category Information to Law Enforcement and other Investigative Agencies SOP (Law Enforcement Disclosures) document and should be followed. Any queries should be directed to the DSP team via dspuhnm@uhnm.nhs.uk.

Original records should not be sent to the Police.

8. REQUESTS FROM SOLICITORS

Solicitors will often make a request for information on behalf of a client. The procedures outlined in the Subject Access Request Standard Operating Procedure must be followed and any queries can be directed to the DSP team via dspuhnm@uhnm.nhs.uk.

If the contact from a Solicitor advises that action against the Trust is intended, the legal team must be advised as soon as possible at Ministries.Office@uhnm.nhs.uk

If the request is in relation to staff grievances or investigations etc. a senior member of the Human Resources Management team should be informed immediately.

If the request is in relation to childcare proceedings, a witness summons should be submitted with the application. Written consent must be submitted with the application and it must be current (i.e. signed and dated no more than 6 months ago).

Original records must not be sent to solicitors. If the Trust's solicitors require original records this should be authorised by the Data Protection Officer who will ensure that adequate security measures are taken and that a copy of the latest episode is retained where applicable.

9. COURT ORDER/AFFADAVIT

Often disclosure of personal information, and most often health records, of the alleged victim of, or witness to, a crime is requested by the alleged perpetrator's defence lawyers, and occasionally by the Crown Prosecution Service or prosecution team. Initial refusal by the Trust to release such records will usually be met by a witness summons being issued by the court (under the Criminal procedure (Attendance of Witnesses) Act 1965 in the Crown Court. The defence legal team are only entitled to have access to confidential material that is relevant to the matters in issue in the criminal trial. They are not entitled to trawl through a patients/victims entire medical history seeking material for cross-examination. Further advice/guidance must be sought from the Trust legal team at ministeries@uhnm.nhs.uk

10 GMC/NMC/OTHER INVESTIGATIONS

It is a statutory requirement to provide this information in relation to a fitness to practice investigation and as such, consent is not required (according to GMC guidance).

There is no harm in the Trust informing the patient that we have received a request from the GMC and that we will be providing copies of their medical records (which are usually sent in an anonymised format) as requested, but we are not obliged to do so and we are not seeking consent for the disclosure. The GMC themselves may inform the patient and seek consent.

The Trust Medical Director/Chief Nurse will be required to review the records relating to a GMC/NMC Investigation (respectively) prior to disclosure, so they will be aware of the investigation as well as the

potential harm that may be caused by informing the patient, so advice should be sought from the Medical Director (as Caldicott Guardian) in liaison with the Data Protection Officer before informing the patient

Where the Trust receives requests for information from organisations other than GMC/NMC as part of an official investigation into public authority activities, for example the Police Complaints Commission, assistance should be provided in the same way that GMC/NMC investigations would be handled. All such requests must be recorded.

On occasion, staff will be asked to check for inappropriate access to a patient's medical record (often the request comes via a complaint but a request to audit the record is valid however it is received). The Trust has a process for handling such requests and this can be found as a flowchart at Appendix 2

11. ACCESS TO MEDICAL REPORTS

The Access to Medical Reports Act 1988 establishes a right of access by individuals to reports relating to themselves provided by health professionals for employment or insurance purposes.

11.1 Rights of the Patient:

Patients have the following rights:

- Their informed consent must be obtained before the report is dispatched.
- They may request that the completed report be retained for 21 days so that they may view the report before it is dispatched. The medical practitioner should not supply the report until this access has been given, unless 21 days have passed since the patient has communicated with the doctor about making arrangements to see the report. Access incorporates enabling the patient to attend to view the report or providing the patient with a copy of the report.
- They may request to see a copy of the report at any time within the next 6 months (so the health professional needs to retain a copy for 6 months after it was written).
- They may wish to discuss the report with the health professional, and to attach a codicil if they feel that the report contains inaccuracies. However, the health professional is not obliged to alter his/her comments if there is still a difference of view.
- They may refuse the sending of the report, so if they subsequently request access to it, the health professional must obtain their consent once again before the report is dispatched.
- Patients have a right to receive information in an ***intelligible*** form, and this is not necessarily in an intelligible form to the applicant. This means that it is not necessary (or a legal obligation) to translate information to another language or to have it transcribed to braille, for example, although staff should consider undertaking this taking into account the costs involved.

11.2 Rights of the Trust:

The Trust has the following rights:

- To make a **reasonable** charge for writing the report, or supplying a copy of the report.
- To refuse to show the report, or a copy of the report, to the patient under the following circumstances:
    - if the report would reveal information about a third party
    - if the report would reveal the identity of a third party who had given the health professional information about the patient for the report (unless that person has consented, or is a health professional).

If a patient requests access to a report, but the appropriate health professional has decided to refuse them access to part of it, it is the responsibility of the appropriate health professional to tell the patient this.

Requests for Medical Reports will be logged by the team handling the request and forwarded to the appropriate consultant/health professional in order for them to write the report. The consultant/health professional dealing with the request should keep the team handling the request informed of progress and the final outcome, including the date the report has been sent to allow the Datix record to be closed.

12. REQUESTS FOR INFORMATION USED FOR BENEFIT ASSESSMENT PURPOSES (DEPARTMENT OF WORK AND PENSIONS [DWP]) OR FOR BENEFITS/TAX FRAUD/EVASION

In order to assess the benefit claims of their client it is often necessary for the DWP to request sight of copies of the hospital records or to have a factual report prepared. This is in order that the claim can be objectively considered. This guidance applies also to any investigation undertaken by an appropriate statutory authority into benefits/tax fraud/evasion, which will usually be handled by Health Records (Ministries)

The request should not be passed on to the patient's General Practitioner. If approached by the DWP for information the responsibility to provide it lies with the Trust and not a third party. The request will therefore be dealt with by the Trust and should be logged as a request, followed up, progressed and the outcome reported and closed on the SAR log being used by the Department handling the request. Any member of staff assisting with such requests must keep the handling team informed of progress and the final outcome. Any third party information should be removed.

Consent to release of information - It is not necessary for the Trust to seek consent to release information to the DWP. The patient will be aware that the DWP may be required to make such requests and the consent from the patient is an integral part of the benefit claim form.

Schedule 2 (para 2) of the Data Protection Act 2018 also allows the disclosure of information where it is required for the assessment/collection of tax.

Requests should be processed within 10 working days of receipt. Prompt and accurate responses are essential if the DWP are to meet their own obligations to their clients. Failure to meet the 10 day "turn round" may result in delay of benefit payment to the client, which could have a personal impact on a patient equally as much as delaying treatment.

13. FURTHER DISCLOSURES

13.1 **MP access to health information about their constituents -** The term "elected representative" covers Members of Parliament (UK, Scotland, Wales, Northern Ireland and EU), local authority councillors and mayors (and their equivalents in the devolved countries). Specific legislation under the Statutory Instrument, 2002, No. 2905, The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002 enables information to be disclosed to elected representatives without contravening the Data Protection Act 2018. However, it does not remove the constraints of the common law duty of confidentiality and as such the common law should still be satisfied (normally by consent) before information is disclosed. See the Section 13 of Model B3 in Confidentiality: NHS Code of Practice (DH 2003) for more information.

13.2 Disclosures to a Local Safeguarding Children's Board (LSCB) during the investigating of a child's death - Local Safeguarding Children's Boards may require access to health records relevant to a deceased child from an NHS body to conduct an investigation/inquiry, although it is more likely that a statement will be requested from the Named Lead for Child Safeguarding (the same will be true for requests relating to Adult Safeguarding). Should records be requested, it is highly likely that the public interest will be served by this process and warrants full disclosure of all relevant information within the child's own records. However, in some circumstances the LSCB may also require access to information about third parties (e.g. members of the child's immediate family or carers). In all cases the LSCB should explain why it believes information about third parties is relevant to its enquiries, and you should use this to consider whether or not there is an overriding public interest to justify the disclosure of the information requested. In cases where you determine disclosure to be in the public interest you must ensure that any information you disclose about a third party is both necessary and proportionate. In ALL cases, the Named Lead for Child Safeguarding should be advised before any information is disclosed.

13.3 **Disclosures to Coroners for the purpose of carrying out an inquiry -** Coroners inquiries are an important part of determining cause of death in a huge number of cases in the UK. Prompt access to confidential information regarding patients and others involved in an investigation is often vital to the reliability of the outcome of an inquiry.

It is the Department of Health's view that the public interest served by Coroners' inquiries will outweigh considerations of confidentiality unless exceptional circumstances apply.

When an NHS organisation feels that there are reasons why full disclosure is not appropriate, e.g. due to confidentiality obligations or Human Rights considerations, the following steps should be taken:

a) the Coroner should be informed about the existence of information relevant to an inquiry in all cases;
b) the concern about disclosure should be discussed with the Coroner and attempts made to reach agreement on the confidential handling of records or partial redaction of record content;
c) where agreement cannot be reached the issue will need to be considered by an administrative court.

The Trust Legal Team will handle all Coroners Enquiries and any request for advice must be made to them.

14. RESEARCH

The UK Policy Framework for Health and Social Care defines research as an attempt to derive generalisable or transferable new knowledge to answer or refine questions with scientifically sound methods. This includes studies that aim to generate hypotheses or test them, in addition to simply descriptive studies. It does not include service evaluation (designed and conducted solely to define or judge current care) or audit (designed and conducted to inform delivery of best care).

In line with HRA advice, normally only a member of the patient's existing clinical care team should have access to patient records without explicit consent in order to identify potential participants for a research project. The care team is categorised as health professionals involved in the diagnosis, treatment and care of a patient, with boundaries defined by patient expectations. However, if the research protocol specifies that a member(s) of the research team may access patient records for this purpose, with justified reason and the research protocol has received NHS REC and HRA approval, then the said member of the research team may access records in line with the protocol.

The Research & Innovation Team should be consulted if any requests for information are received citing research as the basis.

15. TIME LIMITS

15.1 Legally, a formal request for Access to Health Records or Access to Staff Records made under Data Protection Act 2018 must be actioned and completed within 30 days from the day on which the Trust has the necessary information to confirm the identity of the applicant and locate the record. Further information on time limits can be found in the Subject Access Request Standard Operating Procedure.

15.2 Requests for information made under the Access to Health Records Act 1990 are detailed within the Subject Access Request Standard Operating Procedure.

16. CHARGES FOR RELEASE OF THE RECORD

Under the Data Protection Act 2018, you cannot charge a fee to comply with a subject access request. This also applies to access to records of deceased under the Access to Health Records Act 1990

However, where the request is manifestly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request.

You can also charge a reasonable fee if an individual requests further copies of their data following a request. The fee must be based on the administrative costs of providing further copies and staff must be able to itemise and justify the charge.

17. MANIFESTLY UNFOUNDED REQUESTS

Where a subject access request is manifestly unfounded (for example the applicant is using the request to harass an organisation with no real purpose other than to cause disruption), then the Trust is not obliged to answer. However, advice **must** be taken from the Data Security & Protection team and the Caldicott Guardian before any refusal is issued. The ICO Code of Practice provides further guidance and this will be used to determine whether a request is unfounded (When can we refuse to comply with a request?)

18. EXCESSIVE REQUESTS

Whether a request is excessive will depend on its particular circumstances. A request **may** be excessive if it:

- repeats the substance of previous requests and a reasonable interval has not elapsed; or
- overlaps with other requests

The Trust is obliged to try to comply with such a request by making **reasonable** searches for the information and advice must be taken from the Data Security & Protection Team and the Caldicott Guardian before any refusal is issued. The ICO Code of Practice provides further guidance and this will be used to determine whether a request is unfounded (When can we refuse to comply with a request?)

The Trust will review each request individually to determine whether it falls within the definition of 'manifestly unfounded' or 'excessive', however it should be noted that there are limitations in technology making it difficult to meet all requests in full. In cases such as these the Trust will follow the ICO guidance which states that '*you should perform a reasonable search for the requested information'*. The ICO Guidance also states that '*you should make reasonable efforts to find and retrieve the requested information. However, you are not required to conduct searches that would be unreasonable or disproportionate to the importance of providing access to the information'*

19. UNSTRUCTURED MANUAL RECORDS

The ICO guidance states that Unstructured records (non-automated information which is not, or which we do not intend to be, part of a 'filing system' which includes paper records that the Trust does not hold as part of a filing system) is classified as personal data and therefore falls within the remit of the DPA 2018 and this Policy.

The Trust has a duty, in response to a data subject's SAR. However, the Trust is NOT obliged to do so if:

- the request does not contain a description of the unstructured data; or

- The Trust estimates that the cost of complying with the request would exceed the appropriate maximum

The "appropriate maximum" is currently £600 and when estimating the cost of compliance, the Trust will take into the account the cost of the following activities:

- Determining whether we hold the information;
- Finding the requested information (or records containing the information);
- Retrieving the information or records; and
- Extracting the requested information from the records

ICO Guidance advises that the biggest cost is likely to be staff time and it states that this should be measured at £25 per person, per hour, regardless of who does the work.

20. SENDING THE RECORD TO THE APPLICANT

All access responses must be sent via a secure method – in robust packaging and sent via Recorded Delivery if in hard copy or via the Trust's Secure Portal if an electronic disclosure is made. Further details can be found in the Subject Access Request Standard Operating Procedure.

Alternatively, if the applicant requests that their information be sent by e-mail (and this includes any disclosures made to the Police or other investigative agencies), the Trust's secure portal must be used.

21. RESPONSES COLLECTED IN PERSON

Where an access response is to be collected personally by the applicant, then positive proof of identity must be provided before such information is released if the applicant is unfamiliar (evidence of identity may have already been provided when the applicant made the request, see section 6.5, and would not need to be provided again if the evidence provided displays a photograph of the applicant, which is of a true likeness to the person collecting the records).

If these documents are not available a signature from a witness **may** be accepted where the records are being posted to a known address. An appropriate witness would be a person who has known the applicant for a minimum of three years and who is not a relative of the applicant/patient/employee.

22. REVIEW

This Policy is subject to review when any of the following conditions are met:

- The adoption of the Policy highlights errors or omissions in its content;
- Where other policies/strategies/guidance issued by the Trust conflict with the information contained herein;
- Where the procedural or guidance framework of the NHS evolves/changes such that revision would bring about improvement;
- The review date has elapsed;

23. MONITORING

This policy will be assessed against the NHS Digital information governance and security requirements (Data Security & Protection Toolkit) and alongside the DSP Governance Pack to assure the Trust that full DSP requirements are being met

23.1 Associated and Related Procedural Documents

Copies of the associated policies, process and guidance documents can be found on the Trust's Intranet (Policies page)

APPENDIX (1) - REQUEST FOR DISCLOSURE OF PERSONAL INFORMATION

This application must be authorised by an officer senior to the requesting officer and of a rank no lower than Inspector

This request for personal data is subject to the provisions of the Data Protection Act 2018, the Human Rights Act 1998 and the Common Law duty of confidentiality. It is not unlawful to process or disclose personal data in the absence of the consent of, or notification to, the data subject where the purpose is for the prevention and detection of crime or the apprehension or prosecution of offenders, and notification to the data subject would be likely to prejudice the outcome of the criminal investigation/operation. The personal data will be processed for specified purposes only, in relation to the objective of preventing or detecting crime or apprehending or prosecuting offenders,

1)

To: .....

Date: .....

The following request is required to assist in enquiries, which are concerned with and are for the purposes of:

Data Protection Act 2018 – Schedule 11 - Crime Exemption

☐ (a) the prevention or detection of crime; and / or

☐ (b) the apprehension or prosecution of offenders.

Data Protection Act 2018 – Schedule 1 Part 3 and/or Schedule 8 (3) (Vital Interests Disclosure)

☐ Information is required to protect the vital interests of the Data Subject or another person.

2) Please provide information concerning the following individual: (*sufficient detail should be provided to aid location of individual*)

Surname: ..... Other names: .....

Previous/alias name(s): .....

Gender: ..... Age: ..... DOB: .....

Present address: .....

.....

3) Information requested:

4) Brief details of why it is required (i.e. of the investigation / operation)

5) Brief details why the investigation / operation / enquiry may fail without disclosure:

I have substantial grounds for believing that failure to disclose the required information will be likely to prejudice my enquiries because:

6) Has consent been obtained / data subject notified? ☐ Yes ☐ No

Would seeking consent prejudice or compromise the investigation / enquiry? ☐ Yes ☐ No

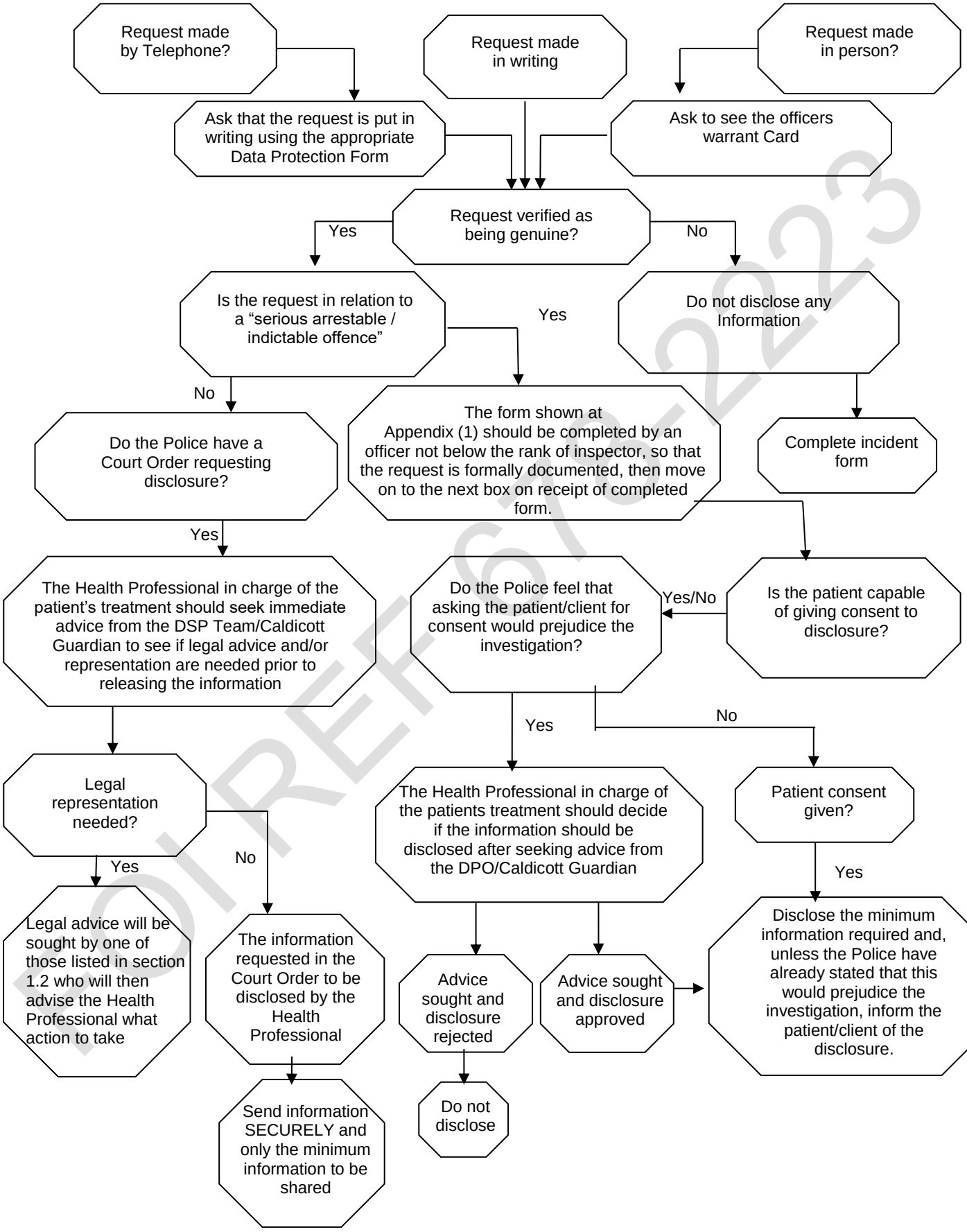
7) I confirm that:

- *the information requested will not be further processed in any manner incompatible with the stated objective;*
- *the information shall not be kept for longer than is necessary for the purposes of the stated objective;*
- *the information will be processed in accordance with the rights of the data subject under the Data Protection Act 1998;*
- appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of and accidental loss or destruction of, or damage to, the information requested; and
- *the details provided are, to the best of my knowledge, correct.*

I am aware of the provisions of Section 55 of the Data Protection Act 1998, regarding the unlawful obtaining of personal data.

Investigating Officer	Rank:
Signature:	Number:
Contact number:	Fax number:
Authorising Officer	Rank:
Signature:	Number:

PROCESS FOR DEALING WITH REQUESTS FROM THE POLICE:



NB: All steps and decisions taken must be recorded on the a Subject Access Request Log

Appendix 2 – Process for Managing Inappropriate Access Audit Requests