NHS
Worcestershire
Health and Care
NHS Trust

SUBJECT ACCESS REQUEST STANDARD OPERATING PROCEDURES

Summary of Key Points

- This procedure deals with the rights of Data Subjects whereby individuals can request access to their Personal Data (PD).
- It applies to all requests for access to PD held by the Trust. This applies to anyone about whom the Trust holds information, including staff, ex-staff, patients and other service users.
- The procedure sets out a framework for the Trust to ensure compliance with GDPR/DPA18 and Access to Health Records Act 1990.
- This document is aimed at informing Trust staff how a Subject Access Request (SAR) to access PD made by individuals or a number of third party sources are dealt with by the Trust. It describes the relevant legislative background governing access requests, together with associated Trust and Department of Health policies. Procedures for processing these requests are explained, from the initial receipt and logging of a request through to clinical / managerial review of the records and disclosure of information.
- SAR's can be made to the Trust to request access to PD recorded anywhere in the Trust, health records, personnel files, complaint files, emails etc.
- GDPR / DPA18 also gives statutory bodies such as the police a right to request information if certain conditions are met, e.g. to assist in the prevention or detection of crime and the apprehension or prosecution of offenders.
- A person does not have a legal right to access the personal information of any other person, however, in certain circumstances these requests can be considered, such as a SAR from a parent or guardian on behalf of young children (under 13)
- The Access to Health Records Act 1990 allows for access to information relating to deceased individuals where certain conditions are met.

NHS
Worcestershire
Health and Care
NHS Trust

Subject Access Request Standard Operating Procedures

Document Type	Corporate
Unique Identifier	IG-033
Document Purpose	This document provides staff guidance on the processing of Subject Access Requests received under the EU General Data Protection Regulation 2016
Document Author	[redacted] Records Manager
Target Audience	Worcestershire Health and Care NHS Trust
Responsible Group	Records Management Group
Date Ratified	22.11.18
Expiry Date	22.11.2021

The validity of this standard operating procedure is only assured when viewed via the Worcestershire Health and Care NHS Trust intranet site. If this document is printed into hard copy or saved to another location, its validity must be checked against the unique identifier number on the intranet version. The intranet version is the definitive version.

If you would like this document in other languages or formats (i.e. large print), please contact the Communications Team on 01905 681770 or by email to WHCNHS.Communications@nhs.net

Version History

Version	Circulation Date	Job Title of Person/Name of Group circulated to	Brief Summary of Change
0.1	27.9.18	Records Management Group Data Protection Officer	Existing Access to Health Records procedures reviewed in line with DH best practice guidelines and GDPR legislation.
1.0	22.11.18	Records Management Group	Approved
1.1	15.4.19	Records Management Group	Appendix 1 clarified to confirm who is responsible for issue of acknowledgement letter to requester.
1.2	14.5.20	IG Team and Data Protection Officer	Amendment to the recording of personal access requests and acceptance of requests made by phone.

Accessibility

Interpreting and Translation services are provided for Worcestershire Health and Care NHS Trust including:

- Face to face interpreting;
- Instant telephone interpreting;
- Document translation; and
- British Sign Language interpreting.

Please refer to the intranet page: http://nww.hacw.nhs.uk/a-z/services/interpreting-and-translation-services/ for full details of the service, how to book and associated costs.

Training and Development

Worcestershire Health and Care NHS Trust recognise the importance of ensuring that its workforce has every opportunity to access relevant training. The Trust is committed to the provision of training and development opportunities that are in support of service needs and meet responsibilities for the provision of mandatory and statutory training.

All staff employed by the Trust are required to attend the mandatory and statutory training that is relevant to their role and to ensure they meet their own continuous professional development.

Co-production of Health and Care – Statement of Intent

The Trust expects that all healthcare professionals will provide clinical care in line with best practice. In offering and delivering that care, healthcare professionals are expected to respect the individual needs, views and wishes of the patients they care for, and recognise and work with the essential knowledge that patients bring. It is expected that they will work in partnership with patients, agreeing a plan of care that utilises the abilities and resources of patients and that builds upon these strengths. It is important that patients are offered information on the treatment options being proposed in a way that suits their individual needs, and that the health care professional acts as a facilitator to empower patients to make decisions and choices that are right for themselves. It is also important that the healthcare professional recognises and utilises the resources available through colleagues and other organisations that can support patient health.

Contents:

1. Introduction

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their Personal Data (PD). It helps individuals to understand how and why the Trust uses their information, and check that the Trust is doing it lawfully. Individuals have the right to obtain the following from the Trust:

- confirmation that the Trust is processing their PD
- what PD data is being processed
- the purposes for which the PD is being processed
- who the PD is shared with
- a copy of their PD

An individual is only entitled to their own PD, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone e.g. a parent). Therefore, it is important that the Trust establishes whether the information requested falls within the definition of PD.

2. Purpose of document

This document is aimed at informing Trust staff how a Subject Access Request (SAR) to access personal data (PD) made by individuals or a number of third party sources are dealt with by the Trust. It describes the relevant legislative background governing access requests, together with associated Trust and Department of Health policies. Procedures for processing these requests are explained, from the initial receipt and logging of a request through to clinical review of the records and disclosure of information.

3. Definitions

Personal Data (PD)

'Personal Data' (PD) means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification

number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Subject

Under GDPR the data subject is a living individual (not an organisation) who is the subject of the PD.

Data Controller

'Data Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of persona data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Subject Access Request (SAR)

GDPR gives individuals rights to be informed what PD the Trust holds about them and, unless an exemption applies, to receive a copy of that information if required. Requests to access this information are known as SARs.

SARs can be made to the Trust to request access to PD recorded anywhere in the Trust, health records, personnel files, complaint files, emails etc.

GDPR / DPA18 also gives statutory bodies such as the police a right to request information if certain conditions are met, e.g. to assist in the prevention or detection of crime and the apprehension or prosecution of offenders.

A person does not have a legal right to access the personal information of any other person, however, in certain circumstances these requests can be considered. Such as a parent or guardian ask make requests on behalf of young children. A parent with parental responsibility can ask for the records of their child or young person. For children who are able to make their own decisions a clinical decision should be documented confirming

whether the child or young person is Fraser competent and whether they should be consenting, or do they object to the parent having the records.

An individual may ask someone else to make a request for them, i.e. a solicitor and will provide consent for the solicitor to request the personal data. Some individuals are not able to provide consent and a Power of Attorney (PoA) may be used. A Health and Welfare Power of Attorney will become active when registered and the person no longer has capacity. There may be occasions when a Property and Finance Power of Attorney may be acceptable if it has been registered and the records relate to matters around finance such as continuing health care decisions.

The Access to Health Records Act 1990 allows for access to information relating to deceased individuals where certain conditions are met.

Third Party

Information relating to another individual and not PD of the data subject for example;

- A parent may apply for access to their child's PD (see definition above). If the young person may be Fraser competent, they should be assessed. The child may have made some reference to his/her parents (the third party) contained within their PD, of which the child did not want to be disclosed. The appropriate health professional may therefore decide to withhold this information from the child's parent.
- A son (the third party) visits the doctor because he is concerned about his elderly mother, who is having problems with memory loss and self-care. The doctor makes a note in his mother's PD record of the visit. If subsequently, for whatever reason, the mother decides to apply for access to her PD, the doctor may withhold any information within her records leading to the identity of the son's visit, unless the son gave his consent to share this with his mother, the data subject.
- A Trust employee makes a reference to access their PD. Within the PD is a prior employment reference from a third party. Trust normal process is to disclose all references to the employees if requested. The reference should be anonymised to

remove any third party information before disclosure, such as the author of the reference.

Representative

- A person who is acting on behalf of the data subject, with the data subject's consent.

Personal Representative

- A person named in the will of a deceased patient as their executor, or
- A person appointed through Letters of Administration as the administrator of the deceased person's estate
- A SAR from anyone other than the data subject (but with the data subject's consent), e.g. solicitor, patient's representative, police, family member, attorney with an active health and welfare or registered property and finance power of attorney, subject to the personal data requested. Please speak with the Information Governance Team if you are in any doubt on whether the applicant is a personal representative.

Attorneys or Court Appointed Deputies

- Someone appointed by the data subject or Court of Protection to act on behalf of the data subject,
- Normally when the data subject is no longer able to do this for themselves, e.g. a data subject who may no longer have mental capacity to make decisions themselves, and if this was for property and finances this can be held even though the donor still has capacity.
- Will have documentation confirming they have been appointed as a *Health and Welfare* attorney for the data subject. If someone had a property and finances PoA there may be some records we would share with them, if relevant to the issues they are dealing with.

- A PoA will be active for health and welfare when the registered person no longer has capacity or for property and finance when it has been registered. Please speak with the Information Governance Team if you are in any doubt on whether the POA can be accepted.

Appropriate Health Professional

- 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, or
- Where there is more than one such health professional, the health professional who is the most suitable to advise on the information, which is the subject of the request, or
- Where there is no health professional available falling within above a health professional who has the necessary experience and qualifications to advise on the information which is the subject of the request.

Advice or enquiries should be directed to the Trust Medical Director, as the Trust Caldicott Guardian.

4. Scope

This procedure deals with the rights of Data Subjects whereby individuals can request access to their PD.

It applies to all requests for access to PD held by the Trust. This applies to anyone about whom the Trust holds information, including staff, ex-staff, patients and other service users.

The procedure sets out a framework for the Trust to ensure compliance with GDPR/DPA18 and Access to Health Records Act 1990.

5. Training/Competencies

The Trust will provide all staff involved in the processing of SARs with appropriate training to enable them to process the requests in line with current legislative requirements. **See Appendix 6.**

6. Responsibilities and duties

Caldicott Guardian

The Caldicott Guardian (Medical Director) is responsible for protecting the confidentiality of people's health and care information and making sure it is used properly.

Company Secretary

The Company Secretary is responsible for protecting the confidentiality of corporate PD and making sure it is used properly.

Data Protection Officer

The Data Protection Officer is responsible for providing advice and guidance about GDPR to work colleagues at all levels, monitoring compliance with GDPR acting as the contact point for the supervisory authority.

Records Manager

The Records Manager is responsible for ensuring all SARs are actioned in a timely manner, and that all staff involved in processing SARs are adequately trained.

Responsible SAR staff

Nominated staff across Service Delivery Units (SDUs) are responsible for the administrative processing, appropriate managers and health professions for the screening and redacting of SARs in a timely manner, in line with this procedure.

Responsibility of all Employees

All employees whether permanent, temporary or contract should be aware of this procedure and adhere to the principles set out. They should all be aware about how to access them.

Responsibility of Records Management Group

The Records Management Group:

- Will ensure that there are effective policies and management arrangements covering all aspects of records management, in line with National guidance.
- Is responsible for raising awareness and coordinating good records management practices across the Trust;
- Promotes training and the implementation of relevant guidance to all employees to protect the confidentiality and security of PD; and
- Receives its authority from the Information Governance Steering Group, and has overall accountability to the Worcestershire Health and Care NHS Trust Quality and Safety Committee. Outstanding issues will be reported to the Information Governance Steering Group

7. ACCESS TO LIVING PATIENT'S HEALTH AND PERSONNEL RECORDS

GDPR/DPA18

This gives individuals or their authorised representative, the right to apply to see certain PD held about them, including health and employee records. These rights are known as 'subject access rights'.

7.1 Who can apply for access?

The Patient

Any patient is entitled access to his or her health records, unless an exemption applies.

Children who are able to make their own decisions and entitled to decide whether they can view their own health records, providing they are judged by professionals to understand their choices and the potential outcomes of sharing information. Case law has established that such a child is known as 'Gillick (Fraser) Competent.

7.2 Employee

Any employee is entitled access to his or her employee records, unless an exemption applies.

7.3 Patient now Living Abroad

When a patient moves abroad, their health records will be retained by the Trust for the recommended period in line with the Information Governance Alliance (IGA) Records Management Code of Practice for Health and Social Care 2016. Patients who move outside the UK are not permitted to take their health records with them; however, they are entitled to request a copy of their records to take the copy abroad with them in an appropriate format.

7.4 Third Parties

A competent patient or member of staff may also authorise a third party to seek access on his or her behalf. For example, patients may authorise solicitors to seek access to their records under the General Data Protection Regulation. The third party must provide proof that he or she is acting on the patient's behalf.

If a third party person is applying for access to the records of an adult who is incapacitated and unable to give consent, information can only be disclosed in the data subject's best interests, and then only as much information as is needed to support their care. Each application will be judged on its merits, evidence of the data subject's wishes prior to incapacitation should always be sought in the first instance, e.g. Health and Welfare PoA in place when we would act on this and not use a best interest process, data subject wishes recorded in the PD.

Enquiries from third parties who do not have explicit consent of the data subject should be directed to write to the Information Governance Team, Company Secretary's Office giving specific details.

7.5 Parental Access to their Child's Health Record

Individuals can apply to see health records if they have parental responsibility for the patient, subject to the approval of the health professional, and the agreement of the child if they are deemed competent to understand fully what is proposed e.g. are Gillick competent.

7.6 Requests for Access by the Police

GDPR/DPA18 –allows (but does not require) PD to be disclosed to assist in the prevention or detection of crime and the apprehension or prosecution of offenders.

Requests from the Police should be submitted on a Personal Data Request form, signed by the requesting officer and countersigned by a senior officer. The data subject should be asked (if possible) for their explicit signed consent to disclose the information, unless this would prejudice the enquiry or court case.

The Crime and Disorder Act 1998 also allows (but again does not require) the Trust to disclose information to the police, local authority, probation service, or health authority for the purposes of preventing crime and disorder.

When reviewing what information should be shared with the police the appropriate clinician should consider;

- Proportionality of the crime under investigation;
- Restricting release of records to those elements that will facilitate the prevention, or investigation of the particular crime detailed in the SAR;
- Whether the best interest of wider society is served by the release of the information.

For the Trust to consider releasing any information without consent, the access request must relate to a serious crime in line with the Crime and Disorder Act 1998 (e.g. murder, rape, etc.), otherwise the Police should be asked to obtain a Court Order or written approved signed consent by the person whose PD will be released. Please see **Appendix 2** - Guidance on Disclosing Personal information to the Police. If you are in any doubt advice should be sought from the Information Governance team.

7.7 Requests by Courts and Coroners

A Court of Law can order disclosure of a patient's health record. These orders should be complied with unless the Trust decides to challenge the order and take the case to a higher Court in an attempt to override the Court's decision. A copy of the Court Order should be requested to ensure that only those records which are the subject of the Order are disclosed.

Courts and Coroners are entitled to request original records under the Coroners and Justice Act 2009. If such a request is received, copies of the records must be retained by the Trust for continuity of care purposes. Coroners normally give sufficient notice for copies to be made, but have the power to seize records at short notice, which may leave little or no time to take copies. If you are in any doubt advice should be sought from the Information Governance team.

7.8 Requests for Access by other Health Care Providers, GPs and Department of Health

Requests may be received via the telephone, email and post for specific information/copies of PD relating to data subjects whom, in the majority of cases, have been treated or employed by the Trust and have moved or have been referred to another health care provider.

NHS England and the General Medical Council confirm sharing of information between health professionals for direct care is an essential part of the provision of

safe and effective care. The Health and Social Care Act 2016 requires that information must be shared within the framework provided by law and ethics and where appropriate with patient consent, see **Appendix 3** - Process to Transfer and Share Patient health records with Out of Area Health Professionals.

How to share information securely?

If you are sharing information with an out of area NHS health care professional, information can be scanned and emailed securely from NHS.net mail address to NHS.net mail addresses. You should send a test email that does not contain any PD and confirm receipt in the first instance. Once you are content the email has been received by the correct person you can arrange to send the PD securely. If you do not have a secure email address to send the information to please contact the Information Governance Team for advice on other secure methods of transferring personal sensitive data. The email address is: WHCNHS.Informationgovernance@nhs.net

If you cannot share information by secure electronic means a photocopy of the relevant information should be made. Original records should not be shared, unless this has been discussed and agreed with the Information Governance Team. The photocopied case notes/summaries should be sent by 'signed' for post and not special delivery or ordinary post in a double bagged taper proof bag. This link gives all the details of how to transfer data – which emails are secure and how to encrypt data http://nww.hacw.nhs.uk/a-z/services/information-governance/secure-email/

7.9 Telephone requests

If a telephone request is received for access, an explanation of the SAR process should be given, and details taken to forward the relevant application form if required. We can accept requests by telephone if you have sufficient information and ID to process the request.

8. Access to Records of Deceased Individuals

8.1 The Access to Health Records Act 1990

This Act provides a small group of people with an unqualified right of access to information contained within a deceased person's health record. These individuals are defined under the Act as 'the patient's personal representative' and include,

- The deceased's executor, or
- Administrator of the estate.

The Act provides 'a person with a claim' arising from the patient's death, which may include those with a financial claim, with right of access to only the information relating to the 'proven claim' to be disclosed. The access request can be considered without the consent of the personal representative and the record holder / service must decide whether the claim exists.

The Trust must uphold any request which the deceased person has previously made regarding non- disclosure of specific information as the data subjects right of confidentiality continues after death.

The Trust accepts these requests can be more complex and need to be judged on their individual merits and where in doubt advice should be sought from the Information Governance Team. Evidence should be obtained from the requester as to their status, such as a Grant of Probate or Letters of Administration.

8.2 Non Statutory rights of access to deceased patient records

There may be circumstances in which certain individuals that do not have a right of access under this Act, request access to a deceased patient's record. A range of public bodies have the authority to request the disclosure of health information, including the Courts, legally constituted public inquiries and various Regulators and Commissions (such as the Audit Commission and Care Quality Commission).

Relatives or carers may have a number of important reasons for requesting information about deceased patients; for example to help them understand the cause of death or providing living relatives with genetic information. The NHS duty of confidentiality continues after the patient's death. Individuals requesting access to deceased patient information must be able to demonstrate a legitimate purpose and in many cases a legitimate relationship with the patient. Each request will be considered on a case by case basis. Please consult the Information Governance Team by email on WHCNHS.Informationgovernance@nhs.net for further advice.

9. PROCESSING AN ACCESS TO HEALTH OR EMPLOYEE RECORDS REQUEST

Nothing in the GDPR prevents doctors or health professionals from giving patients access to their records on an informal and voluntary basis provided no other provisions of the Regulation preventing disclosure are breached. Equally nothing in the Act prevents managers from giving employees access to their records on an informal and voluntary basis provided no other provisions of the Regulation preventing disclosure are breached.

Formal applications for access can be made in writing or by telephone (which includes by email and letter). **See Appendix B for Trust application forms** –

- one for adult patients, or those acting on behalf of the adult patients
- one for access to records of children under 16
- one for employees (former and present), or those acting on behalf of the employee

Forms should be downloaded from the Trust Intranet or Internet Site to ensure the latest version is utilised using this intranet link: Records Management If you require further guidance or have any enquiries, please contact a member of the Information Governance Team by Email WHCNHS.Informationgovernance@nhs.net

The information pathway – access to health or personnel records details key stages of the subject access request process – **See Appendix 1**

9.1 Proof of ID

All applications must be accompanied by two types of identification pertinent to the person making the request (either the patient / employee / permitted third party / representative) e.g. passport, driving licence, birth certificate and additional recent proof of address (within three months) e.g. bank statement, utility bill (mobile phone bills are not acceptable).

Request Received from a third party

When a SAR is received from a Third Party for access to patient records, such as a solicitor, if you have consent from the patient whose records are requested you do not have to request further ID as the solicitor has a duty to confirm ID when agreeing to represent a patient.

If you receive a request for access to a patient or staff member's records from a third party, such as a family member, such as a parent, you will need to satisfy yourself with documentary evidence of their identity and appropriate relationship to the patient. If the request is made by a third party following the death of a patient, you will need to seek sufficient evidence to satisfy yourself that you have confirmed the person's identity and entitlement to request information before you release the records.

Personal Representative

A personal representative is the only person who has an unqualified right of access to a deceased patient's record and need give no reason for applying for access to a record. A personal representative is:

- the person named in the will of a deceased patient as their executor, or
- a person appointed as the administrator of the deceased person's estate

It is appropriate to request a copy of any documentation, such as a will, that will confirm this. However, it is important to uphold any request which the deceased patient may have made regarding the non-disclosure of specific information, even in the case of personal representatives.

People with a claim arising from the patient's death

Individuals other than the personal representative have a legal right of access under the Act only where they can establish a claim arising from a patient's death. This is a separate right to that of the personal representative and may be exercised without the consent of the personal representative.

If a right of access to a record is established due to a claim arising from a patient's death, only information relating to this claim should be disclosed to the applicant. This is to say that there is no right of access to any information which is not relevant to the claim being made.

Who decides whether there is a claim?

It is accepted that those who can prove a financial claim will have a right of access. But in terms of other individuals and other types of claim, the decision as to whether a claim actually exists lies with the record holder. In cases where it is not clear whether there is a claim, please contact the Company Secretary's Office on 01905 681558 to seek legal advice.

Access to PD Evidence Requirements

Type of applicant	Types of documentation required
An individual applying for his/her own records	2 types of ID required, (see examples above)
Someone applying on behalf of an individual (excluding solicitors)	2 types of ID required, (see examples above) which should include patient ID and 2 types of ID relating to third party.
Solicitor applying on behalf of the data subject	Signed consent from the data subject authorising release of PD to the solicitor.
Person with parental responsibility applying on behalf of a young person	Copy of birth certificate (identifying the parent (s) and two types of identification relating to person with parental responsibility (see examples above)
Power of attorney/ agent applying on behalf of an individual	Copy of court order authorising power of attorney/ agent plus proof of patients' identity (see examples above)

Access to PD – Deceased Data Subject

Type of applicant	Types of documentation required
Patient's personal representative	Evidence of being granted Executor of the Will or Administrator of the Estate, and proof of identity (as above)
Person making a claim arising out of the patient's death	Proof of identity (as above) and documented evidence of the legal right of access as a result of the claim

(Please note the copies of any identity paperwork should be destroyed as soon as identity has been checked and request processed.) **Although o*riginal documents are not required, we should record that we have received proof of identity.***

9.2 Time limits for giving access

Once appropriate ID has been received, the General Data Protection Regulation stipulates the information must be provided without delay and at the latest within one calendar month from receipt. This can be extended by a further two months where the request is complex or where there are numerous requests. If this is the case the Data Subject must be contacted within the one month of the receipt of the request and explain why the extension is necessary. The Department of Health has made a policy commitment for health records to be released that this timescale should be 21 days, which is an aspirational timescale for health records and not a legal obligation.

All refusals must be in writing setting out the reasons and the right of the Data Subject if they are dissatisfied with the response to make a complaint to the Patient Relations Team requesting an internal review where a second person will review the documents and provide a second opinion on whether pd should be disclosed.

If Data Subjects are still dissatisfied following the internal review they should be advised they can make a complaint to the Information Commissioner to seek a judicial remedy. Further details of the role and powers of Information Commissioner can be found on the Commissioner's website, www.informationcommissioner.gov.uk

The Information Commissioner's address is:- Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

This is a very short timescale in view of the number of actions that have to take place when an application is made. It is essential that clinicians and all those involved act promptly. Failure to respond within the requirements of the Regulation might be interpreted as meaning that the Trust had something to hide if litigation should later ensue.

Where the applicant does not give sufficient information to identify the data subject, or show that the applicant, if this is not data subject, is entitled to make the application, then a request for further information must be made within 7 days. The time limits for processing the SAR are suspended for the period of time it takes the requester to provide this information.

9.3 Recording the Access Request

Applications submitted on Trust application forms will be directed in the first instance to the Company Secretary's Office, as they carry a single contact address. Upon receipt the Company Secretary's Office will identify the Service Delivery unit (SDU) relevant to the request and it will be passed directly to the appropriately identified administrative service lead for action. Any request for SARs held by multiple services or which do not contain sufficient information to process will be logged by the Company Secretary's Office.

Data Subjects may choose to contact a department or service direct with a request. These can be dealt with by the relevant service themselves and do not need to be passed through to the Company Secretary's Office. Applications sent direct your department/team/service need to be immediately forwarded to your local contact for SARs – see **Appendix 5**.

All applications for the release of employee records should be directed to the Company Secretary's Office where they will be recorded and actioned by the Information Governance Team.

Providing the correct criteria for release of the records have been met the nominated lead will ensure the request is recorded and processed. Examine each SAR individually to assess the impact of the information requested / staff members that need to be contacted restricting the information shared to protect the identity of any allegations or personal information. Consider how widely this needs to be shared to process the SAR whilst protecting the confidentiality of all parties. Email relevant staff to request only information that is relevant to the request from that staff member be sent to IGT Inbox.

All requests must be recorded upon receipt by the service lead contact responsible for access requests, using the Trust SAR Database, link attached SAR Database

Any enquiries regarding access to this Database should be addressed to the Information Governance Team by email. WHCNHS.Informationgovernance@nhs.net

9.4 Acknowledgement of Access to Records Request

The Trust should strive to acknowledge all access to records requests within 48 hours where possible. Template letters are available for this in the shared folder following this link: GDPR Templates

If the applicant has provided either insufficient proof of ID or insufficient details regarding what information they are seeking then the applicant must be contacted within 7 days to request the additional information.

9.5 Requests for X-Rays or Images

With the exception of dental services the majority of X-ray requests from MIU or A&E will relate and should be sent to the Worcestershire Acute Hospitals NHS Trust for them to photocopy and release. Please contact the requester and advise them of the contact details:

Medico Legal, Alexandra Hospital, Woodrow Drive, Redditch B98 7UB.

9.6 Requests for GP Practice records

Requests for copies of health information contained with GP records are not the responsibility of Worcestershire Health and Care NHS Trust. The requester should be directed to apply directly to the Practice Manager at the GP Practice Address for consideration and release.

9.7 Litigation and Court Orders

If the request specifically mentions that litigation is anticipated against the Trust please inform the Trust's Company Secretary (for information only). Note, the request should continue to be processed in the normal way and you should liaise with the Company Secretary's Office to establish whether a copy of the screened records is required at the time of release of screened records to the requester.

9.8 Informing Staff before Disclosure

If a Subject Access Request is received requesting access to patient or staff information that is held electronically on staff shared / personal computer drives or in Email accounts inform the relevant members of staff that a subject access request has been made. Inform the staff members of the redaction process and advise them the decision on whether to disclose rests with the Trust. In the event a staff member disagrees with the disclosure this should be escalated to senior management.

9.9 Clinical or Managerial Review of PD Prior to Release

Health records should be forwarded to the appropriate health professional concerned to ensure disclosure is not likely to cause serious physical or mental harm to the patient, or another person, or if it relates to a third party who has not given consent (where that third party is not a health professional who has cared for the patient) to the disclosure of their information.

Line managers should review employee PD prior to the release of information to the employee paying particular attention to any third party information that may be contained in the record without consent for release.

9.10 Limiting or Denying Access to Health or Employee Information

Schedule 3 of The Data Protection 2018 enables the data controller to limit or deny access to an individual's health record where:

The information released may cause serious harm to the physical or mental health of the patient, or another person, or

Access would disclose information relating to or provided by a third party who has not given consent for disclosure unless:

- the third party is a health professional who has cared for the patient and/or contributed to the health record
- the third party, who is not a health professional, has given their consent to the disclosure of that information
- extra caution should be applied to documents that contain the sensitivity banner of '*Not for Disclosure'* as whilst there should not be a blanket decision to withhold these documents each document should be considered and a decision made in relation to the information it contains. If you are in any doubt please refer to the Information Governance Team.
- 'Serious harm' is not fully defined in the legislation and it is at the discretion of the appropriate health professional to form a view based on their knowledge of the patient and the contents of the health record, whether serious harm is likely to be posed to the data subject or another. If you are in any doubt as to your position you should seek advice from the Information Governance team.

Consideration should be given to the following:

Section 41 of the Mental Health Act 1983 – Courts have interpreted the reference to possible 'serious harm' to the public in the *future* rather than to proven serious harm in the past and have also stated that the risk of harm must be real rather than fanciful or remote. Harm is not simply due to the physical or mental health but also the emotional condition of the individual involved.

If the serious harm exemption is to be relied on the health professional must reach a view on the following issues:

- be of the view that the risk is justifiably real
- be of the view that the risk is more than trivial
- be able to provide justification for the decision which would stand objective scrutiny
- have recorded the reasons for that decision and in case of doubt, be able to record having discussed the issue with a colleague and obtained a second professional opinion

Non Personal Information

When disclosing information it is important that you identify any information that is not personal to the requester, for example:

Disciplinary Hearings may contain non relevant general data such as;

- Introductions,
- Closing Remarks
- Do you want a break
- How has your day been

If members of staff names are mentioned in transcripts these must be anonymised and the staff names replaced with AA, BB etc. It is important to leave in staff job titles so long as individual third parties cannot be identified by doing this.

If a member of staff is acting in an official capacity i.e. Investigating Officer or Human Resources these names should remain in the transcript.

Third Party Information

Information from a non-health professional is classed as 'third party information'. The Trust will only be obliged to disclose 'third party information' where the third party has consented to the disclosure of the information and or where it is reasonable in all the circumstances to comply with the request without the consent of the third party. Where possible the third party should be contacted and advised of the application and given the opportunity to indicate whether they are agreeable to the disclosure.

In determining whether it is reasonable to disclose the information, you must take into consideration all the relevant circumstances, including;

- The type of information that you would disclose;
- Any duty of confidentiality you owe to the other individual (third party);
- Any steps you or the Trust has taken to seek consent from the other individual (third party);
- Whether the other individual (third party) is capable of giving consent; and
- Any express refusal of consent by the other individual.

If the Trust can protect the name and identity of the third party just by deleting the actual name or referring to, for example *'Mr X',* the Trust must provide the information amended in this way.

Information from another Health Professional

Information from another health professional within or outside the Trust, communicated to the Trust as part of the care of the patient is not third party information and may be disclosed unless it complies with a General Data Protection Regulation exemption. The contents of these records must also be reviewed in line with all of the above guidance.

Joint Health/Social Services Records

Where records contain information written by Social Services, permission for disclosure must be obtained prior to release of this information by the Trust from the relevant Social Services staff responsible for that part of the record.

9.11 Redacting / Copying Process

Personnel records should be reviewed and screened by the appropriate manager before disclosure and health and care records should be reviewed and screened by an appropriate health professional before disclosure to:

- ensure that they only include information that is relevant to the request;
- ensure that there is no correspondence or documentation in the PD that is clearly marked 'not for disclosure';
- assess if the disclosure could cause serious harm to the physical or mental health of the patient, staff member or any other person(s);
- remove the identity of other persons who have not consented to the disclosure of the information. The identity of the individual(s) should be scored out with a black marker, ensuring that the name(s) cannot be read.

If redacting copy documents by hand use a black marker pen to cover any information that should not be disclosed. Photocopy the redacted copy ensuring the redacted information cannot be read. Try holding it up to the light to see if you can read the redacted information. If necessary, go over redacted information again and repeat the photocopying process until the redacted information cannot be viewed.

If redacting and sending electronically, **do not** send the source document. Source documents that have been redacted can potentially be "un-redacted" using

specialist software. Print off ensuring the redacted information cannot be read (see above). Scan into the computer before sending the scanned version of the information via a secure method, for example, secure email route or posting out by signed for delivery.

Keeping a log of Redactions

The decision to not release any information that has been redacted due to an exemption should be recorded on a redaction log. This is a requirement of the General Data Protection Regulation 2016 and a good practice in case of any future disputes or reviews. A template redaction log suggested by the Information Commissioner's Office is listed at Appendix 7.

Guidance on making amendments to medical records:

Health records should not be altered or tampered with, other than to remove or correct inaccurate or misleading information. Any such amendments must be made in a way that makes it clear what has been altered, who made the alteration and when it took place.

Information which is clinically relevant must not be deleted from medical records. (For electronic records, information can be removed from display but the audit trail will always keep the record complete.) Amendments to records can be made provided the amendments are made in a way which indicates why the alteration was made so that it is clear that records have not been tampered with for any underhand reason.

Patients may also seek correction of information they believe is inaccurate. There is no obligation for a health professional to amend professional opinion, however sometimes it is difficult to distinguish between fact and opinion. Where the patient and the health professional cannot agree on whether the information in question is

accurate the patient can ask that a statement is included to set out that the accuracy of the information is disputed by them.

Health professionals are advised to provide the patient with a copy of the correction or appended note. Patients also have the right to apply to the Information Commissioner's Office, a court to have inaccurate records amended or destroyed.

9.12 The Release Stage

If information has been limited or denied an explanation for this does not have to be given to the data subject. However, a record of this decision should be noted as part of processing the access to records request.

Applications to View PD

If it is agreed that a data subject or representative may directly inspect a person's PD, they must be accompanied by a health professional in the case of health information or line manager in the case of staff information. Data subjects or representatives should not be allowed to view their records on their own, or to take original records away from Trust property. The health professional or manager should arrange a suitable individual for the data subject or representative to help understand the contents of the records. An appointment should be made with them for this.

The data subject or their representative may request a layperson to oversee the viewing of records; the layperson must not comment or give advice on the content of the record. If the individual raises any queries, offer an appointment with a health professional or manager. If photocopies are required, the healthcare professional or manager should arrange for these to be provided.

Requests for Copies of PD

Copies of the relevant PD may be forwarded to the data subject once approved for release or arrangements made for the data subject to collect in person.

Arrange for the data subject to collect the records

- This is the preferred method within the Trust
- Arrange collection at the earliest opportunity from a Trust site
- Inform the data subject they will be required to produce ID at the time of collection
- Prepare the RECORDS COLLECTION RECEIPT with details of the personal data and ensure that this is completed when the records are collected.
- Scan a copy of the completed template to the SAR Correspondence folder.

Digital transfer of PD – when available

- Arrange to send a copy of the record by secure email ensuring that you dispatch the record from a secure NHS.Net email address to a secure email address such as pnn.police.uk.
- If the person requesting the data has asked for this to be provided in a machine readable, permanent format, full consideration should include consideration of scanned documents, encryption to disc.
- Documents sent electronically must be exported in a secure manner using encryption standards see link for further details. Secure Email
- Ensure separate arrangements are in place for the applicant to ring for the password upon receipt.
- Information and details of secure email routes are available on our Trust intranet site see link for further details: Secure Email

REMEMBER

If you need to send an email containing information that is personal, confidential or sensitive to a non-secured address, then you must:-

- make sure that the email address that you are sending to is the right one

- send a 'test' email first and ask the recipient to 'reply' to confirm their identity and the validity of the email address
- don't include anything in the 'Subject' Field or 'Body' of the email that is personal, confidential or sensitive e.g. patient or staff names
- make sure any documents that are attached to the email are encrypted* with a password
- use 'Options' to Request a Delivery Receipt / Request a Read Receipt
- DO NOT send the encryption password until you have received a reply
- then send the encryption password in a **separate** email or give it over the phone once confirmation has been received

* If you don't know how to encrypt a document then please contact the IG Team at WHCNHS.InformationGovernance@nhs.net

Posting Copies of Records

Copies of PD records sent externally in the post should be:

- In a sealed 'tamper proof' envelope (e.g. self-sealing jiffy bag)
- Addressed to a named person
- Marked 'Private and Confidential'
- Marked 'To be opened by Addressee only'
- Sent by 'Signed for' Delivery

Copies of records sent internally should be:

- In a sealed envelope
- Addressed to a named person and include both Team Name and Team location
- Marked 'Private and Confidential'
- Sent via the Internal Secure Courier

Sending Original Records

Original PD should **not** be sent to any applicant (including solicitors) because of the potential detriment to employees, patients and the Trust if the records are lost. The main exception to this is a request made by Court Order, in which case the originals may be sent and copies must be retained by the Trust, ensuring you follow the release of information arrangements above. Original documents should only be sent to Court if the Order specifically requires original records.

In very exceptional circumstances, it may be necessary to send original notes. In these cases, a copy of the record must be retained in the Trust, details kept of the person that is receiving the notes, along with contact details. These notes must be returned within 21 days and tracked regularly until they are returned.

10. REQUEST TO REVIEW SAR DECISION

There may be occasions where the data subject lodges a disagreement with the clinician or manager's decision on what parts of the PD have or have not been released to the requester.

In these circumstances the requester should be encouraged to supply details of why they disagree with the decision so a review of the original decision can take place. The Trust should strive to acknowledge all requests to review an original SAR decision in writing within 48 hours, where possible, to the requester.

Such reviews should be undertaken by a member of the Information Governance Team in the case of corporate records or in the case of health and care records the Caldicott Guardian, Medical Director, will appoint a different health care professional to ensure all elements of the request have been processed in line with the requirements of the GDPR/DPA18, Access to Health Records Act 1990 or Medical Reports Act 1988.

Once the review has taken place this decision should be communicated in writing to the requester without delay and where appropriate attach any additional PD that the reviewer has determined should be shared with the requester.

The decision letter must contain details of redress available to the requester if they remain dissatisfied with the decision;

- Contact the Trust through its structured complaint handling procedure,
- Contact the Patient Relations Team on 01905 681517 or WHCNHS.PALS@nhs.net
- Contact the Information Commissioners Office on 0303 123 1113

11. FEES

A significant change was introduced on 25.5.18 when GDPR came into force. Most requests can be made free of charge. However, a “reasonable fee” can be charged for further copies of the same information and when a request is manifestly unfounded or excessive, particularly if it is repetitive. The fee must be based on the administrative cost of providing the information and advice must be sought from the Information Governance Team prior to any fees being charged.

12. RETENTION PERIODS

SARs and disclosure correspondence should be retained securely for a period of 3 years on the M: /TeamDrive/SAR folder at which time it should be reviewed and securely disposed of if no longer required by nominated SDU staff who process SARs.

SARs where there has been a subsequent appeal should be retained securely for a period of 6 years on the M:/TeamDrive/SAR folder at which time it should be reviewed and securely disposed of if no longer required.

13. REQUESTS FOR MEDICAL REPORTS

The Access to Medical Reports Act 1988 governs access to medical reports made by a medical practitioner who is or has been responsible for the clinical care of a patient, for insurance or employment purposes. When a report is requested, the patient's written consent is required. A person cannot ask for a report to be written without the patient's knowledge and consent.

The patient is entitled to have access to the report before:

- It is supplied to the employer/insurer (subject to the grounds for withholding access).
- To ask for amendments if they think it is inaccurate,
- To be asked for consent before the report is sent.
- To refuse to allow supply of the report.

If the patient has requested access to the report, the healthcare professional should not supply the report to the commissioner of the report until this access has been given, unless over 21 days have passed since the patient's request without them making arrangements to see the report.

An exception to the rule allowing access would apply where disclosure would be likely to cause serious harm to the physical or mental health of the individual or others, or where disclosure would reveal information about another person – unless they have consented, or that person is another health professional involved in the care of the patient.

Reports must be retained by the medical practitioner for at least 6 months from the date it was provided to the employer/insurer. They should then be securely destroyed. They do not form part of the patient's health record of care.

A reasonable charge may be levied by the Trust for supplying a copy of the report based on the appropriate hourly rate of the person writing the report and the amount of time to draft the report. An invoice should be raised through the Trust finance service.

Reports prepared by other medical practitioners, such as those contracted by an insurance company, are not covered under the Access to Medical Reports Act 1988. They are covered under the General Data Protection Regulation 2016.

14. Monitoring implementation

The Trust will monitor this guidance through the Records Management Group and continued compliance with the NHS Digital Data Security and Protection Toolkit.

The Trust will undertake an annual Information Governance self-assessment using the NHS Digital Data Security and Protection Toolkit.

The Data Security and Protection Toolkit is an on-line self-assessment tool that allows the Trust to measure its performance against the National Data Guardian 10 Data Security Standards. This used to be known as the IG Toolkit.

15. References

The General Data Protection Regulation 2016/Data Protection Act 2018
Access to Health Records Act 1990
Access to Medical Reports Act 1988
Information Governance Alliance (IGA) Records Management Code of Practice for Health and Social Care 2016
Department of Health Confidentiality NHS Code of Practice 2003

16. Associated documentation

Records Management Policy

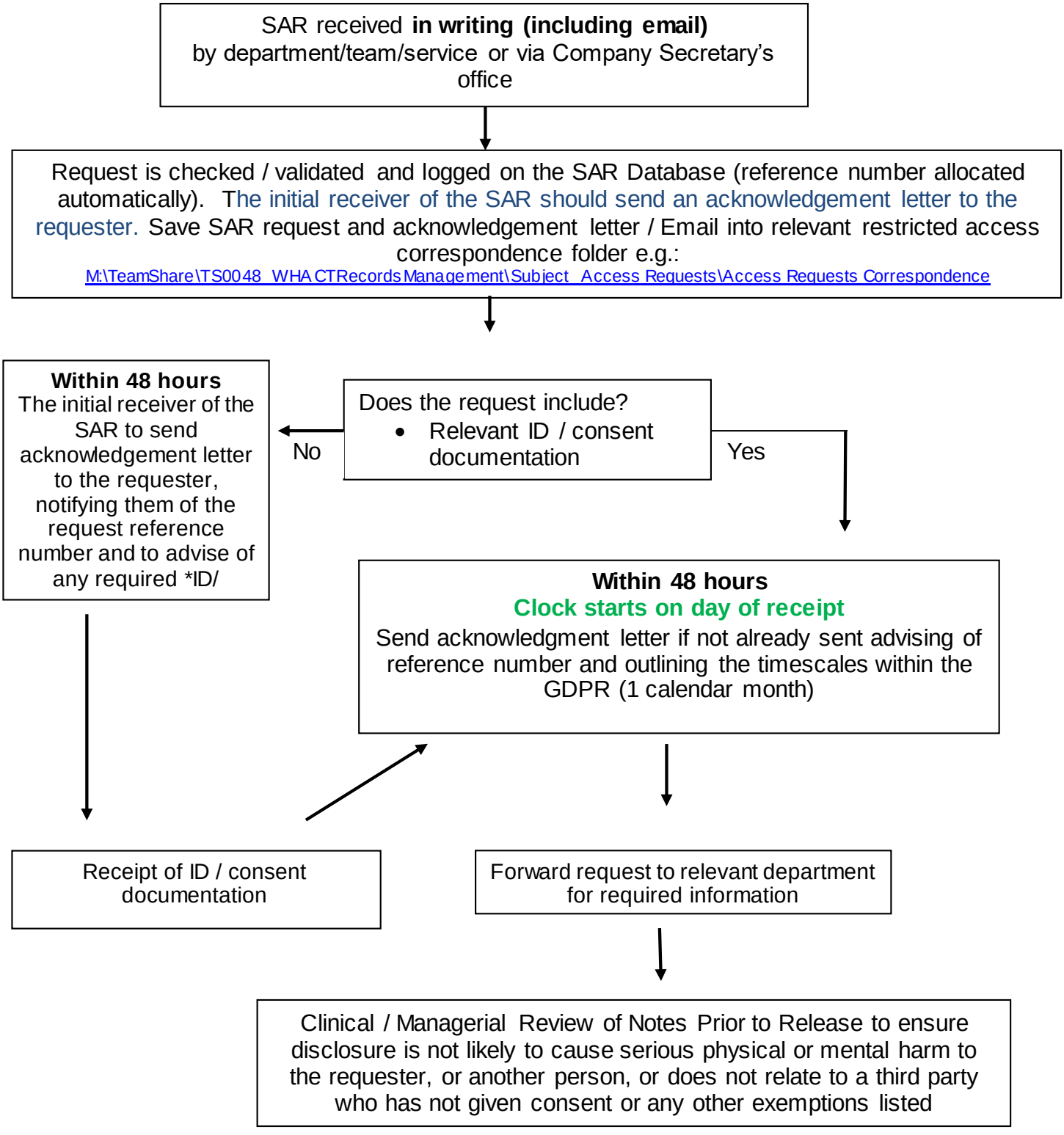
Data Protection Policy

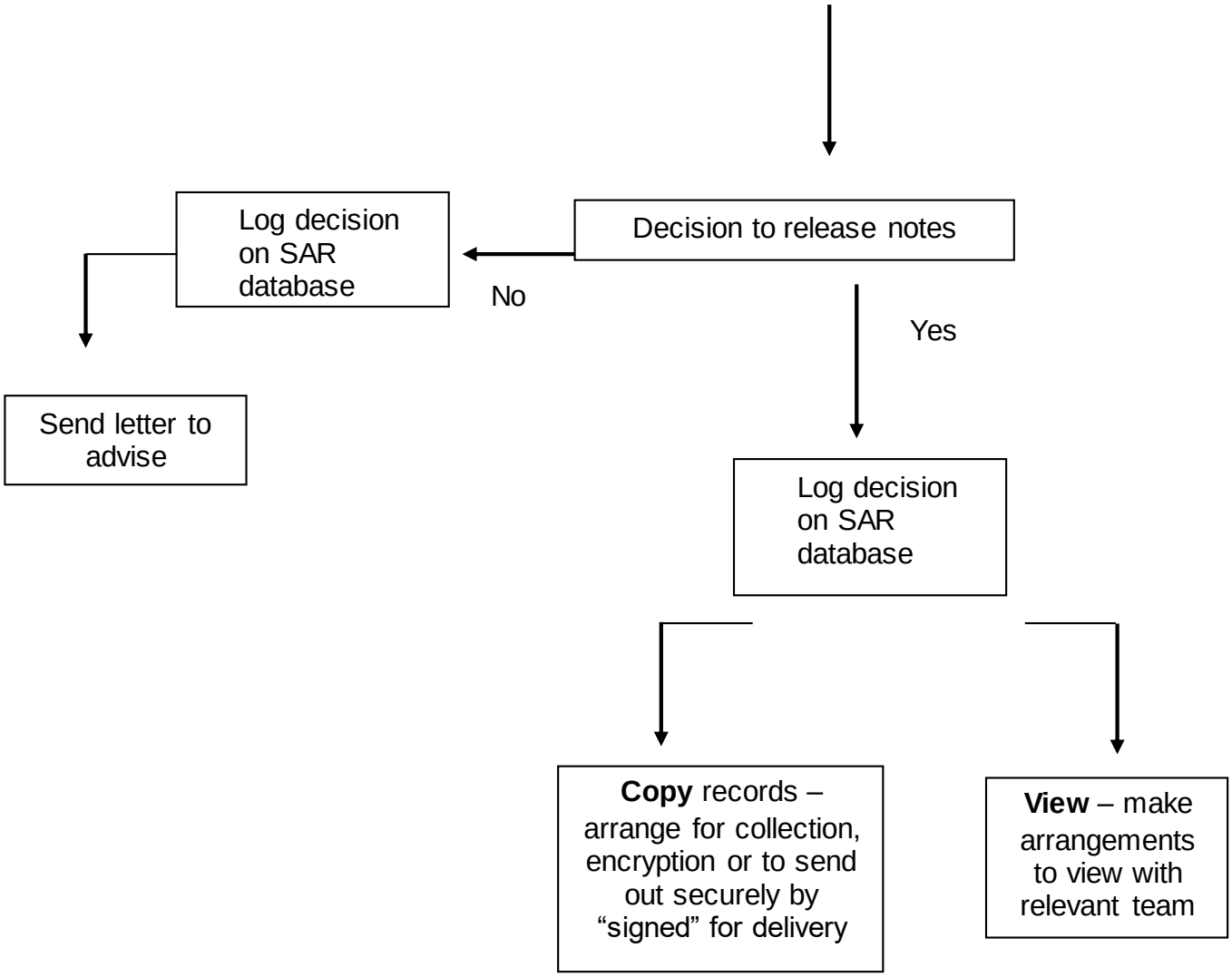
Code of Conduct for Employees in respect of Confidentiality

Clinical Record Keeping Guidelines

17. Appendices

Appendix 1 - Information pathway - access to PD





***Note:** if ID / consent documentation is not received within 3 months this should be noted on the SAR database, send 7 day letter and close on SAR database if no response within 7 days

Appendix 2 – Subject Access Application Forms

Access to Non Health Records

Application for Access to Health and Care Records ((U16))

Application for Access to Health and Care Records (Adults)

Application for Access to Non Health Records

Do You Want Access to your Worcestershire Health & Care NHS Trust Records U16

Do You Want Access to your Worcestershire Health & Care NHS Trust Records

Appendix 3 - Disclosing information to the Police

Guidance on the
Disclosure of Persona

Appendix 4 – Sharing Information with Other Health Professionals

Transfer and Sharing
of Patient health recc

NHS
Worcestershire
Health and Care
NHS Trust

Appendix 5 - Locality/Service Lead Contact Details

Worcestershire Health and Care NHS Trust

Appendix 6 – Access to Records Staff Training Course

Appendix 7 – Redaction Log

Date of Redaction	Document Reference – including page numbers(s)	Details of exempt material	Exemption applied	Reason for justification for exemption	Reviewer comments	Any other comments

Appendix 8 – Frequently Asked Questions (FAQ's)

Q: Who is entitled to request access to patient records?

Patient

Personal representative – solicitor, family member (who has obtained consent), someone with a valid POA for Health and Welfare matters. In some situations a Property and finance POA may be accepted as being relevant to the actions being discharged. For example if the data request relates to an application for Continuing Health Care (CHC) we may consider aspects are relevant for release but also make a best interests decision about other info.

Police

Continuing healthcare

Courts

Coroners

Care Quality Commission

Independent Mental Health Advocates

Court appointed Deputies

Q: Who is entitled to request access to staff records?

Employee

Personal representative – solicitor, family member (who has obtained consent), someone with a valid power of attorney

Courts

Coroners

Court appointed Deputies

Q: What should I do if a request for a medical report is received?

This is not an access request and should be handled by the relevant clinician. The report does not form part of the patient record. Charges should be in accordance with BMA guidance and dealt with in accordance with the Access to Medical Reports Act 1988. Our processes apply to NHS work if the Consultant is undertaking this work as Category 2 work.

Q: What should I do if a request for access to records of a deceased patient from someone who is not named as executor?

The person must have a claim against the deceased person's estate. They must be able to prove the claim and only those parts of the record that are needed for the claim may be disclosed. Seek advice from the Company Secretary's Office.

Q: As a member of staff can I look at my own health records or that of my family or friends?

No. Medical records are confidential. The same rules apply to staff as to the public. In-appropriate access will be investigated as a disciplinary matter and may be referred to professional bodies if the employee is a registered professional

Q: As a member of staff can I request access to my employee file?

Yes. You can request access by speaking with your line manager or submitting a request to the Information Governance Team.

Q: What is the procedure for requests from other NHS organisations, e.g. a hospital, for the purpose of healthcare, particularly if the notes are needed urgently?

- **Do we have to get consent from the patient before disclosure?**

In the case of direct care there is no need for explicit consent but for the purposes of research for example, you would need consent.

- **Do we need to seek permission from the health professional before disclosure takes place?**

  Yes

- **Do the health records have to be screened by a clinician before disclosure?**

  Yes

- **Do the notes have to be copied or should we send originals**

  We should send photocopies

- **If they are originals, how do we ensure we get them back? Do we need to get them back?**

  All original notes sent out of departments to other providers must be tracked and their return regularly monitored and documented

- **Should they be sent by Signed for delivery?**

  Yes, where possible, or secure NHS to NHS email or arrangements made for the requester to collect the records

- **If a patient has been seen by lots of disciplines/services, who is the health professional who screens or gives permissions for the release of the notes? E.g. if the patient has been seen by 2 Consultants and 2 CPNs, do we have to get permission from all the health professionals?**

  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; or where there is more than one such health professional, the health professional who is the most suitable to advise on the information, which is the subject of the request.

  You do not need to approach all health professionals involved, although different disciplines may need to be approached

- **If the health professional who last treated the patient has left the Trust who is responsible for screening the notes?**

  The health professional who has taken over the role, or in the event of a closed service, the SDU lead may nominate an appropriate professional, if there is an issue this should be referred to the Caldicott Guardian

- **What is the procedure for requests from Continuing Healthcare? Do we need to get permission from the health professional to share the notes?**

  Yes. You should seek permission from the last clinician to treat the patient. Continuing Health Care should be sent copies

- **Who is the relevant health professional – our Trust or somebody from Continuing Healthcare**

  Our Trust. The relevant health professional is the person as described previously

- **Do we send original or copies – particularly if the notes are needed urgently?**

  Photocopies, except in exceptional circumstances

- **If they are originals, how do we ensure we get them back?**

  An effective tracking system must be used and regularly reviewed with the requester

Q: How do I deal with requests from solicitors asking if their client has attended a service? And if so, requesting copies of the notes.

a) If their client has never been a patient of ours

Inform them patient is not known to services.

b) If their client is known,

The usual process applies.

Q: What is Parental Responsibility?

A mother automatically has parental responsibility for her child from birth**.**

A father usually has parental responsibility if he's:

- married to the child's mother
- listed on the birth certificate (after 1.12.2003 (England & Wales), 4 May 2006 (Scotland)
- has obtained parental responsibility through a parental responsibility agreement or relevant court order

Special rules apply for same sex couples and advice should be sought from the Information Governance team.

Q: The patient is living abroad. How do they access their UK health records?

Under the General Data Protection Regulation (2016), everyone has the right to apply for access to or copies of their own UK health records, even if they have moved abroad. They should be advised to apply to the record holder(s).

Q: What do I do if I get a request for GP records?

Advise the requester to contact the Practice Manager at their GP surgery as these records are not held by the Trust

Q: What do I do if the patient only wants a copy of a latest letter?

It is always advisable to check exactly what information the patient requires to avoid copying unnecessary documents. A copy of a letter can be screened and released (through an appropriate mechanism) to the requester if ID has been satisfied, for

example patient requests a copy of the assessment letter at their appointment and you have confirmed the ID or are familiar with the patient.

Q: If you think that your request is going to exceed the calendar month limit what should you do?

You should keep in contact with the requester, explaining the reason for this. Try and give an anticipated completion date and advise the Information Governance Team that the request is likely to exceed the one month date.