

Subject Access Request and Disclosure of Personal Data Policy

Policy Domain	IMG
Policy ID	IMG 021
Version Number	9
Author	Les De-Lara
Job Title	Information Governance Lead
First Release Date	01/02/2011
Ratification Date	15/10/2021
Ratified By	IT Steering group
Implemented By	IT steering Group
Audit and Review By	IT Steering Group
Review Frequency	Triennially
Last Review Date	22/09/2021
Next Review Date	01/10/2024

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

This document is the property of the Company and may not be reproduced, by any means, in whole or in part without prior permission of the Company. The document is to be returned to the Company or shredded when no longer required for the agreed purpose.

Table of Contents

1	STATEMENT OF PURPOSE	4
2	RATIONALE.....	4
3	SCOPE	5
4	ROLES, RESPONSIBILITIES AND ACCOUNTABILITIES	5
5	PROCESSING A SUBJECT ACCESS REQUEST	6
6	STAFF TRAINING	14
7	MONITORING AND COMPLIANCE	14
8	EQUALITY IMPACT STATEMENT.....	15
9	REFERENCES	16
	APPENDIX A - SUBJECT ACCESS REQUEST FORM.....	17
	APPENDIX B - ACKNOWLEDGEMENT LETTER (Diagnostics Portal Patients)	19
	APPENDIX C - ACKNOWLEDGEMENT LETTER (All Patients less Diagnostics Patient Portal)	20
	APPENDIX D - ACKNOWLEDGEMENT LETTER (for more information)	21
	APPENDIX E - SAR PROVISION OF RECORDS LETTER.....	22

REVISION SUMMARY

Version	Comments	Author	Date
V1	Implementation of new policy	IM&G Manager	01.02.2011
V2	Amendments throughout the Policy	IM&G Manager	26.02.2011
V3	Policy Review and Update	IM&G Manager	28.08.2013
V4	Policy Review and Update	IM&G Manager	01.03.2015
V5	Policy Review and Update	IM&G Manager	11.05.2016
V6	Policy overall and update including change to 3-year review	IM&G Manager	13.02.2017
V7	Updated policy to include the general data protection regulations	IM&G Manager	27.04.2018
V8	Updated policy to include name change	IG Lead	18/12/2020
V8a	Updated policy to include watermark addition on copies. Providing link or copy of Healthshare’s Privacy Notice and update to sending records electronically.	Operational Support Lead	14/01/2021
V9	Updated policy with new on-line process for SAR using ms forms	IG Lead	22/09/2021

1 STATEMENT OF PURPOSE

This procedure has been written to assist all staff with a responsibility for dealing with requests for personal data from a Data Subject (the individual whom particular personal data is about or their consented agent). These will be known as Subject Access Request (SAR).

2 RATIONALE

This policy provides all those working for or on behalf of Healthshare an overview of the approved process for Subject Access Requests (SARs) and how the records or personal data is to be provided to the applicant.

This policy will clearly define how SARs are to be received and advise what documentation is required as evidence of identification prior to Healthshare processing a request.

Information must be disclosed within one month from the date of receipt of the request, and Healthshare will generally no longer be able to charge data subjects for requesting their information.

Healthshare must act on the SAR without undue delay and at the latest within one month of receipt. If SAR is identified as likely to exceed the 30 day compliance period, requestor is informed of delay and reason for delay by day 25. Healthshare must calculate the time limit from the day the request is received (whether the day is a working day or not) until the corresponding calendar date in the next month.

2.1 Examples provided by the Information Commissioner's Office in interpreting these guidelines are as follows:

- Healthshare receives a request on 3 September. The time limit will start from the same day (3 September). This gives Healthshare until 3 October to comply with the request. If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, you have until the next working day to respond. This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.
- Healthshare receives a request on 31 March. The time limit starts from the same day (31 March). As there is no equivalent date in April, Healthshare has until 30 April to comply with the request. If 30 April falls on a weekend, or is a public holiday, Healthshare has until the end of the next working day to comply. It may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

In certain circumstances personal data may be disclosed, for example, when an exemption is applied under the Data Protection Act (DPA)2018/General Data Protection Regulation (GDPR), there is a legal duty or a Data Sharing Agreement or Protocol is in place or by the request of a bona fide justice system, agency (e.g., The Police or Court). This type of request is not a SAR but it is recommended that each request is individually assessed of the need to disclose the information and document that the information has been released to whom for what reason. The Subject Access Request framework can be used to record and process these types of requests.

2.2 Except in the case of a deceased individual, the Access to the Health Records Act 1990 has been repealed and access to all records for living individuals now comes under DPA/GDPR.

2.3 Individuals (Data Subjects) have rights:

- To be informed whether personal data is processed (which includes being held or stored).
- To a description of the data held, the purposes for which it is processed and to whom the Data may be disclosed.
- To a copy of the information constituting the data.

- To information as to the source of the data.

2.4 This Procedure does not cover in any detail requests for records generated by Coroner's Inquests or Police Enquiries. Please refer to IMG 031 Police Disclosure Policy or the Healthshare Data Protection Officer (DPO) for advice upon receiving such requests.

2.5 This procedure relates to legislation as set out in the DPA/GDPR, covering the use of personal data.

If an application for personal data is made under Freedom of Information for either an alive or deceased person or people, the application should be managed under the Data Protection Act or Access to Health Records Act 2020 and the requestor informed.

3 SCOPE

This policy applies to all Healthshare staff whether permanent, bank or contracted. This policy applies to all requests for access to personal data held by Healthshare. This applies to anyone about whom Healthshare holds information – including staff, ex-staff, service users, independent suppliers, and contractors. This policy will provide a framework for Healthshare to ensure compliance with the Acts and is supported by operational procedures and activities connected with the implementation of Subject Access Requests.

4 ROLES, RESPONSIBILITIES AND ACCOUNTABILITIES

4.1 The Healthshare Group Board

Healthshare Group Board is ultimately accountable for the operation and governance within Healthshare. The Board delegates the development, implementation and monitoring of this policy to the IT Steering Group.

4.2 Senior Information Risk Owner (SIRO)

The SIRO is the Healthshare Board appointed accountable officer ensuring that appropriate information risk management is developed and implemented within the organisation. A number of roles within the organisation including the Information Governance Lead supports this role.

4.3 Caldicott Guardian

The Healthshare Board as is responsible for protecting the confidentiality of a patient and service-user information and enabling appropriate information sharing appoints the Caldicott Guardian. This role will act as a key advisor to the SIRO and is directly supported by the Information Governance Lead.

4.4 Information Governance Lead

The Information Governance Lead is the qualified officer responsible within Healthshare for ensuring that the DPA and GDPR (and relevant other acts) are fully embedded across the company. The role will ensure that Healthshare registration is completed annually and report any issues to the IT Steering Group or SIRO as required.

4.5 Senior Operation Directors

All senior directors within Healthshare have a responsibility to ensure that all records and personal confidential data held by their services is handled in accordance with Healthshare policy and procedures.

These roles will ensure that full support is provided in dealing with requests.

4.6 All Staff

All staff working on behalf of Healthshare have a responsibility to ensure that the aims and objectives of this policy are implemented within their own areas of work.

4.7 External Solicitors

External solicitors can be used where SAR's are required for expert legal advice or to be represented within a court of law.

4.8 Delegated Operational Responsibilities

The Information Governance Lead will oversee the systems and procedures that support the implementation of this policy.

The Information Governance Lead is responsible for:

- Ensuring consent is obtained from the individual for the release of their records, in accordance with the requirements of the DPA and GDPR.
- Providing advice to nominated Senior Directors/SAR Leads on exemptions and exclusions under the DPA and GDPR.
- Liaising with other organisations to process the access request in the event of shared records/data.
- Coordinating the release of the information and ensure that sufficient identification is given by the applicant.

5 PROCESSING A SUBJECT ACCESS REQUEST

5.1 What is a subject access request?

A subject access request is a request made by or on behalf of an individual for the information which he or she is entitled to ask for under Part 2 of the Data Protection Act (DPA) 2018 and Article 15 of the General Data Protection Regulation (GDPR). The request does not have to be in any particular form. Nor does it have to include the words 'subject access' as long as it is clear that the individual is asking for their own data. The Requester does not have to make any reference to the DPA/GDPR, the request may be a valid subject access request even if it refers to other legislation, such as the Freedom of Information Act.

The DPA/GDPR does not specify how to make a valid request. Therefore, an individual can make a subject access request verbally or in writing. It can also be made to any part of Healthshare (including by social media) and does not have to be made to a specific person or contact point.

In Healthshare we request that an on-line SAR form (<https://forms.office.com/r/HKX6dzsuuH>) is completed so it makes it easier to meet the request within the time limit. The form will ensure that:

- The request is structured.
- All necessary details and supporting documents are captured to avoid unnecessary delay.
- Healthshare has up-to-date contact details from the subject.
- A record is kept showing Healthshare met the 30 day regulation.

5.2 Initial action from getting a request for personal data

Healthshare staff members should take the following steps in response to a SAR or a request for information that may be a SAR:

- If you know the requester i.e., a private patient, pass their request to the relevant SAR Lead (*Reception Leads, admin staff or HR*). These members of staff will complete the on-line form for the requester, or they may use an iPad and let the requester complete the form themselves on site under guidance.
- If the requester telephones in, give the requester the link to the on-line form and ask them to complete our on-line form and to upload a proof of identity (e.g., valid passport or driving licence) and inform them that Healthshare will formally respond to their request once their identity has been verified.
- If the requester cannot access the on-line form the SAR lead is to send a copy of the form (Appendix A) to their address for them to complete. The SAR Lead is to complete the SharePoint on-line form.

The relevant SAR Lead will respond to the on-line requests as appropriate. See appendices.

5.3 MS Forms and SharePoint

Healthshare will be using MS Forms with SharePoint for the on-line SAR form. The ms form must be completed for ALL SARs. It can be completed by the subject or a member of staff.

The SharePoint tracking sheet will be held on-line centrally and accessible to all SAR Leads, this will be where the uploaded photo ID documents will be held. The IG Lead will be able to track the request in detail through the service, detailing the date the request was received and when each stage of the request was completed as per Subject Access Request regulations using the backend of MS Forms.

A check must be made of previous requests to ensure that a 'reasonable' time (at least 6 months) has elapsed since any previous request from the same individual. If further clarification is required, staff should contact the Group Information Governance Lead.

The *NHS Code of Practice – Records Management 2016* – states that “Subject access requests must be kept for 3 years after last action and destroyed under confidential conditions” or for 6 years if the request was appealed.

5.4 Letter in Reply

5.4.1 Patients being given access to the patient portal

A letter or email of acknowledgement will be sent to the diagnostics portal requester. The letter must also include the Healthshare's subject access application form link. See Appendix B.

5.4.2 All other patients/requesters

A letter or email of acknowledgement will be sent to the patient. See Appendix C.

5.4.3 Request for further information

If you find that the evidence is not enough you may request further ID to confirm the person. See appendix D

5.5 ID Request

To comply with the law, information relating to the Data Subject must only be disclosed to that person (data subject) or someone with their written consent to receive it.

Adequate steps must be taken to identify the requestor before commencing the work to comply with the request under the act.

Where there is any doubt, proof of identity will be required. Examples of suitable documentation could include copies of:

- Valid Passport.
- Driving Licence.

If the persons cannot access the on-line form and send the originals of these documents, Healthshare must take due care and ensure their safe return. If returning by post, the post must be sent so it is 'tracked and signed for' such as Royal Mail's Special Delivery Guaranteed.

The subject is also expected to provide personal details that enable a search of the records. For example: data subject's name, previous name, address and date of birth.

5.6 Reply Received

When a reply is received from the Data Subject in response to any request for further information, this will be checked by the SAR Lead to ensure that it is satisfactory and adequate to continue the process.

5.7 Search for data/files

The SAR Lead when appropriate will circulate a 'Subject Access Search Memo', to all registered holders of data (i.e., the relevant corporate department or service's team or clinic managers) to search for both manual and electronic information.

The registered holder will be responsible for checking systems (including computer held records), emails, SMS messages and files for any reference, directly or indirectly, relating to the Data Subject. Please remember that the DPA and GDPR does not permit you to exclude information from your response simply because the information is difficult to access.

The Data Subject is entitled to a "legible, understandable and intelligible" copy of the records – and the onus is on the Data Controller (i.e., Healthshare) to comply. At its most basic, this means the information should be understandable by the average person (Subject Access Code of Practice – Information Commissioner's Office). Therefore, if any entry needs to be re-typed – the responsibility for this lies with the relevant Department, service or team. A glossary of terms should be provided to the requester wherever possible.

Copies of the information will be obtained via printing, photocopying and returned to the SAR Lead dealing with the request. In some instances, data is held in an electronic system which you are unable to print off as a document. So, you may need to take screen shots of the information to convert to a PDF document in order to provide a printed copy.

Once the search is complete, the registered holder or holders of data must complete the On-line portal to inform the IG Lead of the outcome – even if no records are found.

5.8 Subject Access Requests – the rights of individuals

The Act ensures the transparency of data processing by obliging data controllers to explain to individuals how their data will be used and by providing the right of subject access. Individuals who request access to their data are entitled to:

- Confirmation that their data is being processed.
- Access to their data.
- Other supplementary information – this largely corresponds to the information that should be provided in the privacy notice.

Individuals also have the right to:

- A description of the personal data of which they are the data subject.
- A description of the purposes for which the data are being processed or are to be processed.
- A description of the recipients of the data.
- Any information available to an organisation on the source of the applicant's data.

5.9 Subject access requests from patients

Where a patient is unable to manage their own affairs then Healthshare will only accept an application by a person appointed by the Courts e.g., under the Court of Protection (or acting within the terms of a registered Enduring Power of Attorney).

Even if a child is too young to understand the implications of subject access rights, data about them is still their personal data and does not belong, for example, to a parent or guardian. Therefore, the child has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a subject access request for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should respond to the child rather than a parent. What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, you should take into account, among other things:

- The child's level of maturity and their ability to make decisions like this.
- The nature of the personal data.
- Any court orders relating to parental access or responsibility that may apply.
- Any duty of confidence owed to the child or young person.
- Any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment.
- Any detriment to the child or young person if individuals with parental responsibility cannot access this information.
- Any views the child or young person has on whether their parents should have access to information about them.

5.10 Data identifying a Third party

Where personal data relating to the applicant also identifies another individual, the applicant's right of access must be weighed against the other data subject's right to privacy. Healthshare should attempt, where practicable, to seek the consent of the third party to the release of their data. Where consent is obtained, the information can be released.

Healthshare Diagnostics using the patient portal are to ensure that the patient is aware that they can share their data via the patient portal and is their responsibility to use this.

In some cases, it may be extremely impractical to attempt to seek third party consent, and in these cases, or where consent has been sought but refused, Healthshare may disclose the other parties' details where it is reasonable in all the circumstances to do so.

In other circumstances, the information may be so significant and of such importance to the applicant that he or she should be allowed access despite the fact that the other individual has not consented to the release of his or her information. In such a case even the release of confidential information may be justified. Reasons for failing to disclose information to the third party must be documented in the event of an assessment by the Information Commissioner's Office.

Where it is not reasonable to supply the third-party data, the information must be redacted to hide any details that may lead to the identification of the third party. It is important to bear in mind that this editing must be applied to any information that might lead the data subject to infer the identity of the other party. Given the sensitive and confidential information that Healthshare holds, if there is any doubt about divulging third party information, legal advice must be sought before making a decision to release information.

5.11 Provision of Information in response to a request

Healthshare will provide to data subjects a copy of their information in an intelligible form and the use of jargon, abbreviations or codes contained within the information must be explained. If the information is terminologically difficult or of a technical nature, Healthshare must offer to 'go through' the information with the data subject to explain the meanings. Healthshare must take into account the provisions of the Disability Discrimination Act 1995 and offer information in large print or Braille format for data subjects with visual difficulties.

Where requested, Healthshare will allow data subjects to view their data. Arrangements will be agreed with the data subject and relevant SAR Lead to facilitate this within the timescales allowed by the Act of 30 days.

Where an access request has previously been complied with under the Act, Healthshare does not have to respond to a subsequent identical or similar request unless a reasonable interval has elapsed since the previous compliance (The Information Commissioner's office has defined a reasonable interval to be 12 months).

Where Healthshare does not hold the personal information requested, we would inform the applicant as quickly as possible.

Records provided are to have a watermark across them such as "released under Subject Access Request", be page numbered and a contents table added to a cover letter with details of Healthshare's Privacy Notice. Then sent by Special Delivery (signed for) to the applicant or secure email, depending on what delivery method the requester has asked for. The records or personal data must be posted in a sturdy 'jiffy' envelope, applicant name and address printed clearly on the front marked Private & Confidential for addressee only and Healthshare address on the back as sender. The envelope must be labelled as per IMG 007 Information Asset Classification Policy. Where possible send copies of records electronically, using encrypted email or by secure portal. Healthshare's Privacy Notice must be included as a link.

5.12 Process Specific Information

Type of Information held by Healthshare

The following list is not exhaustive but does provide an overview of the types of Personal Data that can be requested as part of this policy

- Clinical Records (relating to direct services provided by Healthshare).
- Emails.
- SMS Records.
- Personal Records.
- Minutes of meetings.
- Complaints.
- HR Staff Records.
- Any other structures record.

5.13 Who can apply?

Access to Personal Data can be requested by the Data Subject themselves at any time, however specific other individuals are also capable to make requests:

- Parent/Guardian (who has parental responsibility) of child under 13 (if requesting child's records).
- A representative acting on behalf of the data subject (e.g., Solicitor) with the appropriate written consent.
- Executor of a deceased patient.
- Individual in the event a lasting power of Attorney is in place.
- Any person that has a legitimate claim from the estate of a deceased person (consent should be provided by the relevant delegated authority).
- Any authority where they have a legal basis for investigation (e.g., The Police; and Counter Fraud services).
- Any English Court with a valid Court Order.

To ensure that Healthshare take the upmost care in identifying the legitimacy of any SAR it receives the appropriate documentation including a signed consent form, must be provided.

There are exceptions to this where Police Requests and Court Orders are received which can be provided by the General Data Protection Regulation if requested.

5.14 Shared Records

There are situations where a subject access request involves a health record that is shared between healthcare organisations. Healthshare will consider its arrangements for managing the requirements of the DPA/GDPR and Subject Access requests with its partners as part of any service reconfiguration or development.

The following principles will be followed where this is the case:

- In order to deal with Subject Access requests effectively, the organisation receiving the Subject Access request will take responsibility for processing the request and for obtaining consent or refusal for the release of parts of the record relating to the other organisation.
- Each organisation is obliged to deal with the access request and the authorisation to release the parts of the record in order to ensure the request is processed within the 30-day timescale.
- The period of compliance can be extended by a further 2 months where the request is complex or onerous. In this case the IG Lead and the requester must be informed before the original 30-day period is up and with a reason.
- Each organisation takes responsibility for the access request and joint liability for their release where each organisation has authorised its release.

- If the organisation processing the access request ignores a decision made by the other organisation to exclude data from release and subsequently releases that element of the record, it will accept full liability.
- It is incumbent on each organisation to record the reasons why the release of a record is refused.
- If there is a refusal to disclose the record from the partner organisation, the organisation dealing with the access request should, in their response to the applicant explain the reason for the refusal and refer him/her to the other partner organisation directly if he/she wishes to contest the refusal.

5.15 Police Requests

In the event that Healthshare receive, a request from the Police for records or personal data the Caldicott Guardian and the Data Protection Officer **must** be notified. The same process will apply to any application received with the following exceptions:

- Consent is not essential if the requesting police officer believes that withholding the information will be a serious threat to the public or an individual and it outweighs the patient's interest in keeping it confidential.
- If the records are required in relation to the Counter Terrorism and Security Act 2015.
- Requests will be fully completed within 5 working days.
- In all instances, the request should be signed by a senior police officer, Detective Inspector or above.

5.16 Court Orders

In some cases, applicants that have been unsuccessful in a previous request, or where the information is considered vital in an ongoing court proceeding, it may be required by the Court that either a copy of information is provided and/or that the original documents are made available to the court.

Requests that are received via this route must be passed to the Data Protection Officer for action immediately. The release of this information does not require consent.

5.17 Counter Fraud Investigations

In some cases, an organisation that is delegated by a UK Act of Parliament to carry out criminal investigations, may request Personal Data without gaining consent.

In these cases, when making a request, the applicant must identify which legislation is being used to remove the requirements for consent – these will include the relevant sections in the DPA/GDPR as well as the other pieces of legislation that provide the authority to investigate.

Healthshare as a data controller and data processor will be extremely careful when releasing personal data to such parties and will, following receipt of a request, check that the organisation requesting the disclosure is acting within its powers by asking the applicant to quote the authority on which its power is based.

Healthshare will only accept the request if it is made in writing and it is able to verify the source of the request and any necessary test of prejudice carried out prior to releasing any personal data through its legal channels if necessary.

Law enforcement agencies can request personal information on behalf of and where written consent has been obtained from the individual.

5.18 Consent

In most cases, the provision of consent to share Personal Data will be provided directly by the data subject themselves, usually via a direct request or using a pre-signed authority to release form. However, there are some exceptions to this outlined below:

5.18.1 Insufficient Capacity

Where a person is deemed to have insufficient capacity to make decisions for themselves, a named individual can be appointed by the English courts to act as an advocate for the person. In these cases, this role has the sufficient responsibility to provide consent for release, but evidence of the appointment should be provided at time of request.

5.18.2 Executor / Legal Custodian

Where there is a Lasting Power of Attorney in place (or prior to 2007 Enduring Power of Attorney) a copy of the document declaring the applicant is the 'Attorney' must be provided as proof of entitlement.

5.18.3 Parental Responsibility

Parental responsibility is not a right and particular care should be taken when dealing with requests where children are concerned.

- Mother has parental responsibility

In accordance with English legislation, Fathers do not automatically have parental responsibility for their child if they were unmarried at the time of birth and is not named on the birth certificate of the child. However, they can have Parental responsibility if:

- Married at time of child's birth.
 - Is named on child's birth certificate.
 - Unmarried but registered child's birth jointly with mother.
 - Unmarried but has a joint parental responsibility agreement with the mother.
 - Unmarried but has a joint parental responsibility agreement with the court.

These rules also applies if the child has been adopted.

5.18.4 Others

Next of Kin do not have automatic legal right to Personal Data that are not their own. In the cases of information pertaining to deceased records, the named personal representative (see Executor/Legal Custodian) or a person that may have a claim arising from the person's death.

In all cases, access to Personal Data will only be permitted where relevant consent from the authorised and approved person has been provided.

Healthshare will undertake the necessary steps to verify the validity of an applicant's right to receive any records for a third party.

5.19 Exemptions

There is occasion when records or personal data would not be released to the applicant, either as part of the review of the record (non-disclosure) or fully from the DPA/GDPR. The justifications are provided below:

5.19.1 Reasons for non-disclosing

- As defined in the Access to Health Records Act 1991, based on a health or care professionals' opinion where the provision of records or release of personal data would cause serious physical or mental harm to the applicant/patient or any other person.
- Information related to or provided by, a third party that is included in the record and the third party has not provided consent.

5.19.2 Exemptions from SAR

The following groups are formally excluded when considering Subject Access Requests:

- National Security.
- Publicly Available Information.
- Patients who are part of a witness protection programme.
- Crime and Taxation.
- The disclosure of personal data about more than one individual in response to a SAR, without appropriate consent.

In all circumstances, if the lead member of staff believes that these rules may apply, they should be discussed with the Data Protection Officer and/or the Caldicott Guardian for approval, who will notify the applicant of the decision.

5.20 Can we charge a fee

Not usually. In most cases we cannot charge a fee to comply with a SAR. However, you we can charge a 'reasonable fee' for the administrative costs of complying with a request if it is manifestly unfounded or excessive, or if an individual requests further copies of their data. Refer to the IG Lead for guidance.

6 STAFF TRAINING

To ensure the successful implementation and maintenance of the Subject Access policy, staff must be appropriately informed and trained. Staff appraisal and personal development plans will identify individual needs and Healthshare training strategy will link these into the wider Information Governance Management expectations and requirements of the organisation.

7 MONITORING AND COMPLIANCE

Monitoring/audit arrangements	Methodology	Reporting		
		Source	Committee	Frequency
Performance against the Data Security and Protection Toolkit	Annual audit	On-site audit	IT Steering Group	Annually
Review of the policy <ul style="list-style-type: none"> • legislative changes. • good practice guidance. • case law. 	ITSG Meeting	Sign off on ITSG	IT Steering Group	Annually or when required
Confirmation all SARS were met within 30 days and if not,	Annual Audit	On-Line form	IT Steering Group	Annually

Monitoring/audit arrangements	Methodology	Reporting		
		Source	Committee	Frequency
that due process was followed				

8 EQUALITY IMPACT STATEMENT

During the development of this policy the Company has considered the needs of each protected characteristic as outlined in the Equality Act (2010) with the aim of minimising and if possible remove any disproportionate impact on employees for each of the protected characteristics, age, disability, gender, gender reassignment, pregnancy and maternity, race, religion or belief, sexual orientation.

If staff become aware of any clinical exclusions that impact on the delivery of care an incident form would need to be completed and an appropriate action plan put in place

8.1 Equality Impact Assessment

The Company aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. The Equality Impact Assessment tool assesses the impact of this policy.

		Yes/No	Comments
1.	Does the document/project affect any group less or more favourably than another on the basis of:		
	• Disability	No	
	• Sex	No	
	• Race	No	
	• Age	No	
	• Gender Reassignment (including transgender)	No	
	• Sexual orientation	No	
	• Pregnancy & Maternity	No	
	• Other identified groups	No	
2.	Is there any evidence that some groups are affected differently?	No	
3.	If you have identified potential discrimination, are there exceptions valid, legal and/or justifiable?	NA	
4.	Is the impact of the document/project likely to be negative?	No	
5.	If so can the impact be avoided?	NA	
6.	What alternative is there to achieving the document/project without impact?	NA	
4.	Can we reduce the impact by taking different action?	NA	

Completed by:

Name Les De-Lara	Position IG Lead	Date Completed: 04/03/2021
----------------------------	----------------------------	--------------------------------------

9 REFERENCES

REFERENCES	<ul style="list-style-type: none"> • General Data Protection Regulation • Access to Health Records 1991 • Access to Medical Reports 1990/2020 • DPA 2018 • Data Protection (Subject Access Modification - Health) Order 2000 • Information Commissioner Guidance – Subject Access requests • Records Management: Code of Conduct Part & Part 2 • Mental Health Act 2000
RELATED POLICIES	<p>IMG 002 General Data Protection Assurance Strategy and Management Framework</p> <p>IMG 007 Asset classification Policy</p> <p>IMG 030 Disclosure to the Police Policy</p>

APPENDIX A - SUBJECT ACCESS REQUEST FORM

Under the Data Protection Act (DPA) 2018 and the General Data Protection Regulation (GDPR), you are entitled to obtain from Healthshare, confirmation as to whether we are processing personal data concerning you, as well as to request details about the purposes, categories and disclosure of such data.

You can use this form to request information about, and access to any personal data we hold about you. After you fill in the email address field you will receive an email with a link to up-load your photo ID (Please check your spam/junk mail as it may get caught in there).

*For patients requesting their data in person at point of exam, your identity will be verified by the receptionist/admin team who **MUST** complete **Personal Details and Verification** sections below.*

For patients requesting images by post / email, staff please record details of one photo ID provided (e.g., passport / driving licence) details in verification section. Staff may request further ID if they have any doubts on the person requesting being who they say they are.

Please ensure you upload to Healthshare a copy of either your passport or driving licence.

A. Personal Details (These are the details of the person giving consent):	
Full Name:	
Contactable telephone No:	DOB: ___ / ___ / _____
Email Address:	
Confirm Email Address:	
Method you would like to receive your data: Email or Post:	
Full Address: (Please include full postcode)	
Previous Address if changed since treatment started: (Please include full postcode)	
B. Verification:	
Please ensure you send a copy of a photo ID e.g., Passport or Driving License	

PLEASE DO NOT SEND ORIGINALS

To be completed by requester: Please confirm details of ID provided:

C. Specific Details of Data Requested (including dates where possible):

E. Representatives (only complete if you are acting as the representative of a person requesting the data)

(Please Note: We may still need to contact the person where proof of authorisation or identity has not been provided)

Representative's Name:

Telephone No:

Relationship to Patient:

Representative's Address:

Email Address (If different to section 1):

I confirm that I am the authorised representative of the named person:

Representative's Name:

Signature: _____

F. LEGAL STATEMENT

I confirm that I give my consent for Healthshare to liaise with any other bodies that form part of the investigation into my complaint.

I confirm that the information I present on this form is correct and accurate and I understand that to falsify any information may render me liable to prosecution:

Full Name: _____ [print name]

Signature: _____

Date: ____ / ____ / ____

GUIDANCE NOTES: PLEASE READ BEFORE COMPLETING THE FORM

If you require access to the data we hold about you, you are able to request copies from Healthshare by completing the application form above.

1. The form above gives Healthshare the right to disclose records pertaining to the name as detailed in the Personal Details section of the consent form.
2. If you have had a Diagnostic Scan Healthshare will send you a link to a portal where you will be able to see both report and your Images. It is your responsibility to share those images to any 3rd party such as solicitors you may

wish to.

3. The Personal Details section of this form identifies the recipient of the records, this must be completed at all times. It also provides Healthshare with the personal details required to identify the records requested. In addition, a legal statement must be signed in all cases in the Legal Statement section.

4. The Representatives of the person requesting data for family member section is for any family members who are requesting on behalf of the family member. This part can be ignored if nobody else forms part of the requested records.

5. In order to ensure that the records are provided to the correct person applying for them, Healthshare needs a form of evidence about the identity of the person applying. The evidence must be supplied via the email that has been sent with instructions to upload the photo ID. A clear copy of a passport or driving licence (photo id) is required to be uploaded.

6. Proof of identification is not required in cases where a complaint is being investigated as the appropriate consent will already have been obtained.

7. If you have any questions or need to contact anyone about any part of this form, please email us at: DPO@Healthshare.org.uk.

APPENDIX B - ACKNOWLEDGEMENT LETTER (Diagnostics Portal Patients)

(Use company headed paper)

Our ref: You're Ref:

<<Date>>

PRIVATE & CONFIDENTIAL

<<Name>>

<<Address>>

Dear Sir/Madam

RE: NAME

We are in receipt of your request for records received on XXX and associated identification documents.

You can now use a patient portal that can be access by selecting this link (or pasting it in to your browser) where you will find your reports and images.

<https://forms.office.com/r/HKX6dzsuuH>

If you wish to share these with a 3rd party, please use the portal to do this, select share and follow the instructions.

Please do not hesitate to contact us if you have any queries regarding your application.

Yours sincerely

Name

Position

APPENDIX C - ACKNOWLEDGEMENT LETTER (All Patients less Diagnostics Patient Portal)

(Use company headed paper)

Our ref: You're Ref:

<<Date>>

PRIVATE & CONFIDENTIAL

<<Name>>

<<Address>>

Dear Sir/Madam

RE: NAME

We are in receipt of your request for records received on XXX and associated identification documents.

A search for your records has now commenced and we anticipate you having receipt of these within 30 calendar days, [DAY] [MONTH] 2021.

Once your records have been collated, they will be sent as indicated by your choice of email or post

Please do not hesitate to contact us if you have any queries regarding your application.

Yours sincerely

Name

Position

APPENDIX D - ACKNOWLEDGEMENT LETTER (for more information)

(Identification required and use company headed paper)

This is to request more information

You're Ref:

<<Date>>

PRIVATE & CONFIDENTIAL

<<Name>>

<<Address>>

Dear Sir/Madam

RE: NAME

We are in receipt of your request received on XXX.

In order to respond to your request, we now require the following from you:

- Your full name and date of birth
- A copy of the picture page of your passport or driving licence
- Consent from XXX** *[Delete if no consent required]*

Healthshare operates under strict patient confidentiality regulations. Therefore, I would be obliged if you could obtain consent from XXX and ask that they complete and sign the enclosed consent form. *[Delete this paragraph if no consent required]*

Once we are in receipt of the above you can expect to receive a response within approximately 30 calendar days.

Once your identification documents have been provided Healthshare will commence a search of our records, these will then be posted to you either by Royal Mail Special Delivery or email depending on your choice. The Royal Mail deliveries must be signed for either at the delivery address or at the Royal Mail Sorting Office.

Please contact us on the number above if you require any help with your application.

Yours sincerely

Name

Position

APPENDIX E - SAR PROVISION OF RECORDS LETTER

(Use company headed paper)

Our ref: You're Ref:

<<Date>>

PRIVATE & CONFIDENTIAL

<<Name>>

<<Address>>

Dear [NAME]

Re: NAME

This letter includes a table of contents providing a description of the records provided. Please let me know if we can be of any further assistance.

Yours sincerely

Please find enclosed a copy of your records held by Healthshare

Name

Position

/enc

Page Number	Date of Record	Type of Record	Description