Information Legislation Requests
under the General Data Protection Regulations (GDPR), Data Protection Act 2018, UK GDPR 2019 and Access to Health Records 1990

REMEMBER: Fill in the request Audit Log

September 2025: Version 7_01
Author: Senior Requests Officer

Table of Contents

Section A- Overview

What is a subject access request?

The GDPR/ DPA18 and UK GDPR gives individuals the right to be told what 'Personal data' an organisation is processing (holding) about them and, unless an exemption applies, to receive a copy of that information. The Access to Health Records legislation allows for access to information regarding deceased individuals where certain conditions are met.

They do this by making a data subject right of access request, which might be received by any member of staff. The request can be in writing (including e-mails) or verbally, if someone makes a request by telephone or in person you should ask them to put it in writing or supply copies of the Trusts application forms for clarification and identification purposes. The request can be very broad (such as, 'give me a copy of all the information you hold about me') or it can be very precise ('give me a copy of the letter you wrote about me yesterday').

A person has no automatic legal right to access the personal information of any other person. However, parents and guardians[1] can make requests on behalf of young children, and an individual can ask someone to make a request for them, e.g. a solicitor. We require the person making the request on behalf of another person to provide us with information about themselves. This will help us decide if it is appropriate to release the personal information.

If the request is not for personal information, it must be treated as a Freedom of Information requests and passed to the Freedom of Information Officer at bsmhft.foioffice@nhs.net .

[1] The person who has parental responsibility, as set out in the Children's Act 1989.

1. Logging the Request

All Trust documentation will state that initial requests for access to personal information, regardless of if this is for Corporate or Clinical, should be sent to Information Requests at Trust Headquarters who will start the process, should a request go elsewhere the process will be to:

- If the request is received electronically forward the request and all attachments to bsmhft.informationrequests@nhs.net on the day the request is received.

- If the request is received by post, date stamp the request and then send a scanned copy to Information Requests at bsmhft.informationrequests@nhs.net and confirm on the email that the original has been confidentially destroyed.

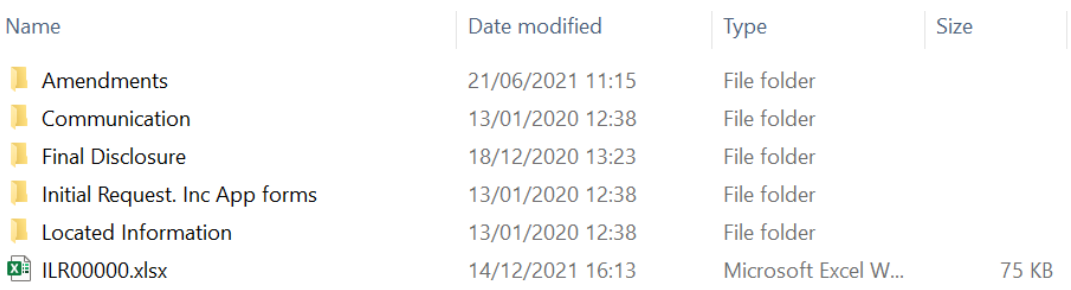
It is important we log **all** requests and keep track of them so that we can monitor our progress and response time compliance.

- All requests will be allocated the prefix ILR and assigned a reference number to the request using the master log available at network location: Z:\Data Protection Requests\ILR Master Log

- Complete the master log for the new request including:
  - Category of ILR (column D)
  - Date Request Received (column O)
  - Request Allocation (columns F and G)
  - Name of data subject (column X)

- **DO NOT** enter any details into the grey boxes (columns H to J, M and N and finally T and W) as these will automatically populate based on the information that is entered into the master log.

- Create a new folder and set of sub folders on the network for the new request (copy and paste the template folder and rename with the reference number you gave the request: Z:\Data Protection Request\Procedural *(ILR####).* Rename the folder to include the reference number taken from the master log, e.g. ILR0021. The sub folders will include the following:
  - Folder – Amendments
  - Folder – Communication
  - Folder - Final Disclosure
  - Folder - Initial Request, inc. app forms
  - Folder- Located Information
  - Excel Document: 'ILR####'



Name	Date modified	Type	Size
Amendments	21/06/2021 11:15	File folder	
Communication	13/01/2020 12:38	File folder	
Final Disclosure	18/12/2020 13:23	File folder	
Initial Request. Inc App forms	13/01/2020 12:38	File folder	
Located Information	13/01/2020 12:38	File folder	
ILR00000.xlsx	14/12/2021 16:13	Microsoft Excel W...	75 KB

REMEMBER: Fill in the request Audit Log

- Keep the following kinds of information in the folder and sub folders:
  - Copies of any correspondence between yourself and the data subject, between yourself and any other parties, including any correspondence with staff internally.
  - When saving records please ensure that the file title follows the format YYYYMMDD…… (date correspondence sent/ received, followed by a brief description)
  - A record of your decisions and how you came to those decisions on the request audit log. (You will need to save copies of any information provided by a clinician).
  - Copies of the actual information sent to the data subject, for example if the information was anonymised keep a copy of the anonymised version that was sent to the data subject.
    - This would need to be stored in the 'Located Information' folder.

- Enter initial basic information into the audit log for the request (a template will be in the template request folder) i.e. date received, staff member dealing with request, plus any actions taken to date, e.g. which clinician the request has been sent to.

  NB; This must be completed and held electronically.

- Scan in the initial request for information (if applicable- may already be in electronic format) and save in the 'Initial Request' folder using the following format YYYYMMDDInitialRequest (date being date request entered Trust- not the date you received it necessarily).

- If you have enough information to continue pass the request to the Records Team for continued processing via the generic email bsmhft.SAR@nhs.net
  - Save the email in the request folder in the Correspondence folder using the following format YYYYMMDDPassedToILR. Make sure it is saved in 'Outlook Message Format' (drop down in save as box).

2. Requests for information – Clinical Information

All clinical/ health records requests must be forwarded to the most recent or current clinician to query if the records need to be reviewed prior to disclosure to ensure a serious harm test is met. Serious harm relates to data that would be likely to cause serious harm to the physical or mental health of the data subject (patient) or another individual. If we are advised that a harm test is not required, the clinician must provide a rational as to why.

The Data Protection Act 2018 defines the appropriate health professional undertaking the test as '…. *the health professional who is currently or was most recently responsible for the diagnosis, care, or treatment of the data subject in connection with the matters to which the data relates*'[2]

[2] Schedule 3, Part 2, Section 2 (1), Data Protection Act 2018

In order to meet the Trusts requirements under Article 15 of the GDPR the Trust will initially **only** provide electronic records from the electronic patient record (EPR) unless the requester has stipulated what information they explicitly require.

Please note that the requester **will** retain the option of obtaining further records that the Trust may hold following the initial disclosure. The requester will need to advise what additional records they require.

In-patient Records

The records collated for this type of request will be those available in Rio under

- '*In-patient Management*'
    - '*Admission – Consolidated Notes*'

Out-patient/ Community Records

The 5 most recent Care Plans, Risk Screening and all Progress Notes will be provided.

At this stage **no** information contained within the folder '*Clinical Documentation*' will be collated to form part of the discloser.

- Log request as per '*Logging the Request*' section.
- Validate the request as per '*How to Determine if it is a Valid Request*' section
- Send email (SAR03) to the most recent/ current treating clinician to advise that a request has been received, what information is being considered for disclosure and that the clinician has 10 working days to advise Information Requests if there are any objections to the information being disclosed to the requester.
- Day 11, if no response has been received from the Clinician the request will be escalated to the Clinical Director for the area for them to confirm if there are any objections to the information being disclosed.
- Day 23, if no response has been received from either the Clinician or Clinical Director the Trust will assume that there are no objections to the records being disclosed and the Records Team will prepare the documents for disclosure by day 30.

3. Requests for information – Objections

- If there are **no objections** to the records being disclosed to the requester the Records Team will be advised via email and they will proceed to disclose without a clinical review. A rational for this decision must be provided.
    - The Records Team will complete an assurance check prior to the records being sent to ensure that all the information relates to the data subject and no erroneous information for example misfiles are disclosed. Records staff names will be redacted from any reports that are run for the disclosure for security and privacy purposes.

- The Records Team will collate the information for disclosure within the 'Request Binder' and edit this to reflect the documents being disclosed and ensure that the front cover is completed.

- If there **are objections** to the disclosure the information will need to be clinically reviewed. At this stage the Records Team will be advised via email to bsmhft.SAR@nhs.net for the Team to collate the records and send word versions with 'Track Changes' switched on for the clinician to review and amend.
- Where the records are being reviewed by the most recent/ current treating clinician any information that needs to be redacted/ withheld must clearly marked using 'Track Changes' in Microsoft Word. A rational for any redactions will need to be applied along with the exception to be used from the UK GDPR and DPA18.
  - The clinical review would need to be completed by day 23 of the request and returned to the Records Team
    - The exact date that the review will need to be completed by will be included as part of the review notification email received from the Records Team.

4. Requests for information – Current Inpatient

From time-to-time requests will be received from data subjects or their representatives who are currently within an in-patient setting. In this instance the Responsible Clinician must be contacted to ensure the patient is well enough to receive the information or has the capacity to agree to someone to act on their behalf – NB: this excludes requests where the representative is a solicitor.

In the above situation the process will be….

- Request to access records received by Information Requests….
  - Log request as per instructions in 'Logging the Request' section and put the request on hold.
  - Information Requests to email the Responsible Consultant to ask them to confirm if the patient is well enough to make the application/ receive the records before proceeding further.
    - If confirmed that the patient is **not well enough/ lacks capacity** to make the application/ receive the records then Schedule 3, Part 2, Paragraph 5(1) of the Data Protection Act 2018 will be used to exempt the data and close the request.
      - Complete template letter SAR13 and send to requester.
      - Ensure audit log is updated and letter saved and close request.
    - If confirmed that the patient is **well enough/ has capacity** to make the application/ receive the records, the request is to be taken off hold and passed to the Records Team via bsmhft.SAR@nhs.net to continue with the process.
    - Please see 'Requests for information – Clinical Information' for further details

5. Requests for information – Clinical Documentation

Clinical Documentation will not automatically be collated to form part of a disclosure, unless a specific request for this data is received. Where Clinical Documentation is

required, the Records Team will be responsible for initially collating and reviewing this data.

Following review if the if the clinical documentation is deemed to be….

- **Non-contentious**/ low risk, for example appointment letters/ clinic letters these are to be reviewed by Records Team and disclosed within the 30 days' timeframe.
  - The Records Team will complete an assurance check prior to the records being sent to ensure that all the information relates to the data subject and no erroneous information for example misfiles are disclosed.
- **Contentious**/ high risk for example Safeguarding reports the most recent/ current treating clinician is to be contacted and the Records Team do not disclose at that time.

- For high risk/ contentious clinical documentation email (SAR03) to the most recent/ current treating clinician to advise that a request has been received, what information is being considered for disclosure and that the clinician has 10 working days to advise Information Requests if there are any objections to the information being disclosed to the requester.

- Day 11, if no response has been received from the Clinician the request will be escalated to the Clinical Director for the area for them to confirm if there are any objections to the information being disclosed.

- Day 23, if no response has been received from either the Clinician or Clinical Director the Trust will assume that there are no objections to the records being disclosed and the Records Team will start to prepare the documents for disclosure by day 30.

6. Requests for information – Paper Care Records

Copies of paper Care Records will not be automatically included in the application unless the request specifically asks for historical information, pre EPR.

Where historical information is required the process will be the same as if the information was held on the EPR – refer to 'Requests for information – Clinical Information' section with the exception that the records will be collated by the Digital Records Management Team at Barberry who will send them to the Scanning Bureau for the documents to be scanned onto OnBase. The Records Team will download the records from OnBase to forward to the Clinician for review and or disclosure.

7. Requests for information – Healthcare Provider

Requests from Healthcare Providers are split into 2 types of requests. Those from the NHS and those from Private Healthcare providers. For NHS requests **only**, Clinical review and consent is not required.

Please note only information contained within the EPR will initially be considered for disclosure. If a copy of the paper Care Record is required, the requesting Healthcare Provider must state the clinical need for this historic information. If paper records are to be disclosed the request must also be copied to the Digital Records Management Team

at Barberry who will send them the records to the Scanning Bureau for them to be scanned onto OnBase. The Records Team will download the records from OnBase to forward to the requester.

NHS

- *Log request as per* '*Logging the Request*' *section.*
- *Validate the request as per 'How to Determine if it is a Valid Request' section and confirm what information is being requested.*
- Applicable information from the EPR to be saved to '*Located Information*' in the request folder.
- Records Department to send information to Healthcare Provider
- The Records Team will complete an assurance check prior to the records being sent to ensure that all the information relates to the data subject and no erroneous information for example misfiles are disclosed.

Private Healthcare Provider

- Log request as per 'Logging the Request' section.
- Validate the request as per 'How to Determine if it is a Valid Request' section and ensure legal basis is present for requesting the record and that the request details what information is required.
- Send email (SAR03) to the most recent/ current treating clinician to advise that a request has been received, what information is being considered for disclosure and that the clinician has 10 working days to advise Information Requests if there are any objections to the information being disclosed to the requester.
- Refer to 'Requests for information – Clinical Information' on how to proceed with request.

8. Requests for information – Police inc. DBS

Requests from the Police are not uncommon and frequently include a third-party material form or countersigned WA170 which details justification of the why the information would be provide without prior knowledge of the Data Subject. When a request is received without the third-party material form the professionals involved may be obliged to share confidential information in line with "public interest". The BMA advises that *'Disclosures in the public interest based on the common law are made where disclosure is essential to prevent a serious and imminent threat to public health, national security, the life of the individual or a third party or to prevent or detect serious crime[3].'*

The third-party material form must always be sought if the justification does not meet the threshold for disclosure as an individual's right to confidentiality can be overruled to protect the public interest[4]

The request will be logged and processed in-line with 'Logging the Request' section.

The team should always be provided with a completed dated and countersigned third-party material form or WA170 for West Midlands Police (or equivalent from other Police forces).

[3] BMA, Confidentiality and disclosure of health information tool kit – Card 10: Public interest
[4] HSCIC, A guide to confidentiality in health and social care (September 2013), p.20

Should the Trust choose to disclose information consideration will need to be made to ensure only information that is necessary, relevant, and not excessive is included.

8.1 SFR Medical (Streamlined Forensic Reporting)

Only for victims of crime where medical records are required as evidence of a crime. SFR Medical (sfrmedical.westmidlands2@nhs.net or sfrmedical.plo@nhs.net) will email a third-party material form to the Information Legalisation Requests mailbox, it must be stated on the form that it relates to a victim of crime. If the perpetrator box is ticked, then this must be returned to the police and then the police will need to follow the Appendix 5 process as below.

All requests from SFR Medical must be logged on the SAR master log. Please see Point 1 – Logging a Request for more information. When completing the master log please ensure that the category of 'POL – Medical Records' is selected and in requesters Name that 'WMP SFR Medical' is inputted.

8.2 Appendix 5 and 6

These requests are received from the police requesting specific information relating to an individual's capacity at the time of an assault on any emergency worker. The request and applicable form are received via email. The Appendix 5 form needs to be forwarded to the Clinician Team for completing as agreed with the Trust.

It is important we log **all** Appendix 5 requests and keep track of them so that we can monitor our progress and response time.

Appendix 5

- All Appendix 5 requests must be logged on the Appendix 5 log and an acknowledgement email sent.
- Forward the initial request to the Clinician/Team (copying in DPO Kirstie McMillan Kirstie will review the request If Kirstie feels that it is not appropriate, then she will let the ILR team know. The request is then closed, and Karen Barker (police contact) will need to be advised, so she can speak to the officer. If the request is valid Kirstie will not come back to you, so proceed as you currently do) asking for confirmation of completion and justification if declined. Advise to return the completed for to the Information Legalisation Requests for disclosure by SAR Team.
- Calander entry for two weeks to chase if no response close on the third week and advise the Police of the closure and the contact email for the Clinical Team.

Solihull HTT have asked that we mark these requests as urgent to ensure timely action.

Appendix 6

These should be completed by the clinician at the time of the incident and is linked to the Eclipse system. Should our team receive one please forward to the Responsible Clinician/ Team. These requests **do not** need to be logged.

9. Caldicott Requests

These requests are dealt with on a separate tab on the Master Log and comprise of requests for information from a variety of requesters who require information urgently and usually come without the consent of the data subject. We use the Caldicott Principles[5] to determine how we respond to these requests.

When received these requests are moved to the Caldicott Email inbox bsmhft.caldrequests@nhs.net. to be dealt with by the SAR team. We then ensure that the requester has a valid and secure email address and then log the request onto the SAR Master Log. A search for the requested information is then performed and if available disclosed to the requester. As these types of requests are of an urgent and/or sensitive nature we aim to have these responded to as a priority.

Examples; -

Missing Person: recent engagement, last contact with the Trust. These requests require a note adding to the service users RIO record by the responsible SAR officer.

Section 117 Aftercare: responsibility enquiry

Social Services: is an individual known to the Trust

10. Requests for information – Staff/ Corporate Records

Staff and Corporate records include but not limited to.

- Physical Personnel Files
- ePersonnel records
- ESR data including ARDs and RMS'
- Information held with HR re grievance/ daw
- Information with payroll – SBS
- Interview scoring, shortlisting, references and recruitment in general held on TRAC
- Information regarding phone calls, texts and emails
- Information regarding 'swipe card' access for staff
- Counter Fraud investigations
- Injuries at work

When a request is received check OnBase, via OnBase Queries to see if there is an electronic ePersonnel record available, if not go to Line Manager if leaver go to the Records Department at The Barberry.

If the file is with Line Manager, they will send the original for copying to ILR Officer and they will review and return to Line Manager. ILR Officer will send a email to the Line Manager to advise of the request and timeframes.

[5] The Caldicott Principles - GOV.UK.html

If the request is for other data, the ILR Officer liaise with the appropriate department and request this e.g. SSL for swipe card access etc, this information will need to be reviewed before sending.

For applications received from staff where they use their NHS.net email account no further ID will be sought, and the disclosure will be done via their NHS mail account. For staff who have left or chose to use their personal email address then the Egress process will be followed, and further ID will be required before proceeding. Where staff use a third party to request their information e.g. a Solicitor, Egress is not required but valid consent from the staff member will be needed before proceeding.
It is acknowledged that staff/ corporate requests can be complex in nature. On review of what information is being sought and the number of departments involved the request may reach the threshold of 'complex'. In these instances, the requester will be written to be advised that the request is being extended by a further 60 days and will be advised of the new breach date. The Trust aims to advise the requester within 7 days if the Trust classify the request as complex as per ICO guidance, although this is not always possible.

When is a request complex?
Whether a request is complex depends upon the specific circumstances of each case. What may be complex for one controller may not be for another – the size and resources of an organisation are likely to be relevant factors. Therefore, you need to take into account your specific circumstances and the particular request when determining whether the request is complex.
The following are examples of factors that may, in some circumstances, add to the complexity of a request. However, you need to be able to demonstrate why the request is complex in the particular circumstances.

- Technical difficulties in retrieving the information – for example if data is electronically archived.
- Applying an exemption that involves large volumes of particularly sensitive information.
- Clarifying potential issues around disclosing information about a child to a legal guardian.
- Any specialist work involved in obtaining the information or communicating it in an intelligible form.
- Clarifying potential confidentiality issues around the disclosure of sensitive medical information to an authorised third party.
- Needing to obtain specialist legal advice. If you routinely obtain legal advice (for example, where lawyers are responsible for responding to, or reviewing SARs), it is unlikely to be complex.
- Searching large volumes of unstructured manual records (only applicable to public authorities).

Requests that involve a large volume of information may add to the complexity of a request. However, a request is not complex solely because the individual requests a large amount of information.
Also, a request is not complex just because you have to rely on a processor to provide the information you need in order to respond.

The ILR Officer will record on the audit log that the above has taken place and save a copy of the email or letter to the log.

Should the ILR Officer not receive a response within **10 workings days** of notifying of the request, the ILR Officer will send the first chase email to individual or department who are sourcing the information. A copy of the chase email will be saved to the log for reference.

A second chase reminder will be sent 5 **workings days later (week 3 of the active request)**. If the information is not received by the specified date it could result in the request breaching the statutory timeframe. If this occurs an Eclipse incident form must be completed by the ILR Officer for auditing and monitoring purposes.

Once the information is received and reviewed by the ILR Officer it will be securely disclosed by the SAR Team with a covering letter to the requester and the request closed on the audit log.

11. Requests for CCTV Footage

Check if valid request. Valid request must come Police, Insurance Company for damage to cars/ property or a senior in the Trust giving valid justification.

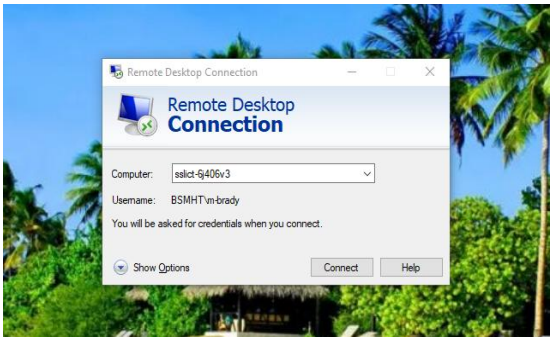
ILR Officer will check the retention period for the site and then will acknowledge to advise if footage is potentially available and then request any further documentation if required e.g. WA170 from Police or consent from the Insurance Company.

Any requests for CCTV must be forwarded to the Information Requests Team at bsmhft.informationrequests@nhs.net who will undertake to process the request/ review CCTV footage.

- Information Requests to log the request as per instructions in 'Logging the Request' section and establish where the CCTV footage can be obtained from, as detailed below.
- The Information Requests Officer will secure and review the footage to determine if there are any confidentiality issues to be considered.
- Footage will be securely released to the requester if appropriate. If the footage does not show the incident being investigated Information Requests Officer will advise the requester and as a general principle not disclose any footage.

Accessing CCTV on the remote PC
Only the Head of Records, Senior ILR Officer and ILR Officer can access CCTV.

Firstly, access to remote desktop connection is selected from the start up search bar.



The computer name is sslict-6k406v3 your username will be shown underneath you will then be asked to connect.

You can connect using One Sign or your allocated Username and password.

ILR Team do not have access to footage from the following sites;

- Barberry
- Oleaster
- Zinnia

Contact Alex Nichols of Equans alex.nicholls@equans.com for above sites.

- Email Alex Nichols alex.nicholls@equans.com to ask for the footage to be downloaded. Equans will arrange for the disclosure and log this as per their process and advise the ILR Officer when it has been collected so the Trust can close the request.

Griffin Video System SOLAR CAMHS[6]
This is a stand-alone CCTV system put in place to record interactions in family therapy.
The lead contact to obtain this footage is Lindsay Murcott lindsay.murcott@nhs.net

NB: It is a breach of GDPR to destroy information once a formal request has been received.

12. Requests from NMC, GMC, Coroners Court, Medical Examiners[7] & Court Orders

Should the Trust receive requests from the NMC, GMC, Coroners Court, Medical Examiners[8] or a Court Order for records, these need to be logged and processed in line with 'Logging the Request' section. Please note however these requests do not come under the remit of Article 15 of the GDPR and do not need to be reviewed either by a

[6] Solar CAMHS DPIA
[7] Coroners and Justice Act 2009
[7] Written statements - Written questions, answers and statements - UK Parliament
[8] Access to Health Records Act 1990

Clinician or Line Manager prior to disclosure as they are reliant on other legislation [9]for the mandatory disclosure of records. The records will require an assurance check prior to disclosure to ensure that all the information relates to the data subject and no erroneous information for example misfiles are disclosed. Consideration will also need to be made for 3rd Party information regarding GMC and NCM requests, as this may need to be redacted/ withheld.

13. Requests to HMP Birmingham from inmates (including relatives), Solicitors and Probation Services.

Requests for records held on HMP Birmingham SystmOne must be forwarded to the Trusts Information Requests Team (ILR) at bsmhft.informationrequests@nhs.net and logged (as per section 1. Logging the Request).

The ILR team is responsible for.

- Ascertaining the validity of the request and whether consent and or identification is required.
- The ILR team will advise of the ILR reference number by emailing the HMP Birmingham shared mailbox (bsmhft.hmpbirminghamhealthcare@nhs.net) **and** Business Manager
- The ILR team will acknowledge receipt of the request with the requester.
- The ILR team will deal with all subsequent correspondence relating to the request.

HMP Birmingham is responsible for.

- Collating the required records
- Forwarding the records to the prison GP for review and authorisation to release the documents.
- HMP Birmingham will copy in the ILR team to all correspondence for audit and query purposes.

The ILR team will follow the process for standard requests by adding a calendar date to chase for an update and sending this to the shared HMP mailbox and Business Manager 10 days from receipt of the request copying in Dave Austin Head of HealthCare HMP Birmingham for awareness again adding a calendar reminder for day 20 of the request. On day 20 of the request if no response or records are received, we will advise the requester of a possibility of breaching the statutory timeframe, again copying in Dave Austin.

In the event of a breach HMP will complete an Eclipse incident and advise ILR team of the reference number.

14. How to Determine if it is a Valid Request

A valid access request is one which:

- provides all the information you require to identify the person and locate the information the person wants.

- provides sufficient information to verify the data subject's identity or right to be a legal representative.
- If someone is acting as a legal representative, they will need to provide their clients consent to do so. Consent is not considered valid if it is older than 6 months unless we are aware of a regular solicitor for their client, and they have requested within the last twelve months.

Following receipt of a request and logging (in any format) …

- Send the requester a copy of the ILR application pack (**only** if there is not enough information to progress request, *Forms 1 or 2, and Guides 1&2*) and/or initial response letter *(ILR1a or ILR1c)*
- Save the letter you have sent in the request folder on the network, in the 'Communication' folder using the following format: YYYYMMDDAck (date being date letter sent e.g. 20201230Ack). Make sure it is saved in 'Outlook Message Format' (drop down in save as box).

14.1 How to determine if a request is reasonable and proportionate.

The GDPR states that if we believe a request to be manifestly unfounded or excessive, we can apply an exemption and challenge or decline the request. In these circumstances we would look for:

Manifestly unfounded.

- The request is malicious in intent and is being used to harass an individual or the Trust.
- Specifically targets individuals.
- Systematically sends requests e.g. every week or daily.

Manifestly excessive.

- The context of the request and nature of the relationship with the requester and the Trust
- If the request repeats previous requests and a reasonable time period has not elapsed
- If the request overlaps current open requests
- Available resource and the volume of information requested.

We would look at each case individually and consider each request in the context that it is made. If a request seems to fall under this remit when received the management team should be advised and after consultation the decision will ultimately be made by the Senior ILR Officer.

15. Locating the information requested

Based on your knowledge of the business area, decide where the 'personal data' about the individual concerned might be held, and locate that information. Ensure you read the

request fully to see if the requester has asked for any specific information, such as a clinical team or a date range.[10]

You may need to search other central filing systems, personal records, shared drives, the Intranet or private filing systems of individuals, e.g. email accounts. If necessary, you must ask colleagues to search their personal drives and e-mail accounts or contact ICT for assistance.

NB: An individual has the right to ask for access to ALL personal information an organisation holds about them regardless of age, format, or location.

15.1 Where may records be held? – Consider Rio, IAPTus, CarePath (Illy), IFOS, Iron Mountain, PALs, Complaints, HR etc…
When staff start to collate electronic records the name of the staff member running the report/ consolidation is sometimes captured and displayed, for example on Progress Notes and Inpatient Consolidation Notes in Rio. In these instances, the name of the staff member who ran the report should be redacted prior to disclosure.

The Trust has been live with electronic patient records since 2011 so most of the clinical data will be held electronically however sometime the paper records are required as part of the application. In these instances.

- If notes are with the clinician; do not request back.
- If notes are **not** with relevant clinician, email Barberry Records that the paper records are required, and Barberry will locate and arrange for the record to be scanned.

…Send notes (paper or electronic (if applicable)) with permission request letter and staff guidance to relevant Clinician (*letter SAR3, NHS02 or A2HR02) and Guidance on Reviewing Information*.

NB: Remember to inform the reviewer if the requester has narrowed down the request as they only need read this section.

16. Screening/ Reviewing the Information for Disclosure

Review the information in line with Trust guidance – please note that this is the responsibility of a suitable Clinician for a client/ ex client request or a line manager for an employee/ ex-employee request. *Someone who has a professional understanding of the information!*

[10] We only need to release what the requester has specifically asked for, so if they have narrowed the request down it is likely to save you time.

Please refer to '**Guidance on preparing information for disclosure under the GDPR'** for full information on what reviewers need to consider, how to apply rules and practical examples of applying the rules.

NB: The Head of Information Governance / Head of Records are available to offer advice where needed from a legal perspective, but the final decision is the responsibility of the reviewer.

Reviewing Information- Steps:

- Reply to notification email to advise if a review is required (this allows you to detail what information you believe can and cannot be disclosed and provide reasons).
  - Where a review is not required a rational for this decision **must** be provided
  - Where information is to be withheld a reason **must** be provided in all cases. This is so we can justify our decisions should we ever be asked to.
  - The review must be completed within 21 days of receipt of the records.
  - If there are any problems with responding, please ensure that the appropriate person(s) is informed as soon as possible.

NB: Refer to Section B and Section C for guidance on managing third party information.

17. Confirming the Identity of the Requester

Before disclosing any personal information, you must verify the identity of the data subject.

Whilst it is important that you do not send copies of personal information to people who are not the data subject, you must not appear obstructive. The legislation requires you to take "reasonable measures" to verify the identity of a data subject. You should keep a record of what measures you take (use the audit log).

You can often verify their identity from their circumstances e.g. address, signature. To gain verification of the data subjects' identity or the requester's ability to request the information you must (use letter SAR1a/ SAR1c/ A2HR01 as applicable):

- Write to the individual and ask them to send you copies of their ID (see guide 2)
  - Save the letter in the 'Correspondence' file using the following format: YYYYMMDDIDRequest.

18. Replying to the Request/ Disclosing Information

When information is ready for disclosure:

- Check we have received ID and are happy with it- if no ID has been received write to requester again using letter SAR19 or A2HR07 and advise if you have not received a response by a certain date, we will assume that the records are no longer required, and the request will be closed.
  - Save the letter in the 'Correspondence' file using the following format: YYYYMMDDIDRequest2.

NB: If you are not happy following the ID checks inform the Head of Records.

Preparing the Information:

- Download/ scan all the information in line with wishes of reviewer **(a copy of the disclosure must always be retained by the Trust).**
    - The reviewer will have 'tagged' any information they wish to be withheld, e.g. comments inserted into Word or Adobe Acrobat.
    - If any information needs withholding (redacting) this should have been highlighted via 'Track Changes' in which case apply all changes and save the amended/ redacted version. If changes are highlighted in Adobe Acrobat use the redaction tool provided with the software.
        - All requests should be disclosed using the Request Binder. Information will have to be merged to the binder and the index and cover sheet updated. For more information about the Request Binder please see refer to applicable appendix.
        - When ready the information can be disclosed either via email from the SAR mailbox or via OneDrive.
        - In some circumstances the requester will ask for a paper copy to be sent as opposed to electronic. In these instances, the Request Binder and covering letter are to be printed and the request sent via Recorded Delivery or UPS. In either instance a tracking ID must be entered on the audit log.

Disclosing Information:

No information being disclosed:

- If no information is being released to the requester complete letter SAR13 or A2HR04 and send to the reviewer in an email to sign off and send. (save email in 'Correspondence'3folder using the following format YYYYMMDDNILResponseForReview)
    - The reviewer must let the relevant person know and provide a copy when the letter has been sent.
    - Save the letter in the 'Final Response' folder of the request folder using the following format: YYYYMMDDFinalResponseNIL.

Full or Partial Disclosure of Information

- If information is being released the information will need to be merged into the Request Binder and the index and cover sheet updated. For more information about the Request Binder please see refer to applicable appendix.

- When disclosing via email use the ILR mailbox and write a covering letter to the requester (use letters SAR10, SAR10a, SAR11 or A2HR05 depending on circumstances) and attach the Request Binder.

- When disclosing via OneDrive note in the comment section '*Please see link for the disclosure of ILR1234. Please be advised that you will need to open/save/download the information within 5 working days as the link will be unavailable after this date*' For more information about OneDrive please see refer to applicable appendix.

- In some circumstances the requester will ask for a paper copy to be sent as opposed to electronic. In these instances, the Request Binder and covering letter are to be

printed and the request sent via Recorded Delivery or UPS. In either instance a tracking ID must be entered on the audit log.

- Enter the finished date of the request on the audit log, the completion date is the date the information is emailed, posted sent via OneDrive.

- Retain a copy of all the information that is released, whenever any information is withheld or not. We need this should requests ever be queried.
    - The information to be disclosed should be merged to the Request Binder and saved in 'Final Disclosure' in request folder.

- Save a copy of the closure letter in the 'Correspondence' file using the following format: YYYYMMDDClosure

19. Managing Breached Request

All requests that have breached the statutory timeframe of 30 days will be included in a desktop review. The review will be undertaken quarterly and be led by the Senior Requests Officer and Head of Records to identify any trends or gaps in process. The outcome of the review will be forwarded to the DPO and Medical Director for awareness and be included in the half yearly report to the Information Governance Steering Group.

Near Breach Procedure.

To prevent unnecessary timeframe breaches, the ILR team on a weekly basis review the master log to determine if any requests are due to breach the statutory timeframe within the next 10 days. This is achieved by filtering the master log to all active requests. Any requests due to breach within 10 days are investigated to ensure the normal process has been followed. The tracking log and correspondence are checked and any chases for updates are actioned if applicable.

20. Closing the Request

Once the request has been completed it needs to be closed.

- Email the Information Requests mailbox (bsmhft.informationrequests@nhs.net) to inform that the request has been closed.
- On the master log Information Requests will enter the date closed. Information Requests will update the master log and enter the date the request was closed for any closed requests for non-clinical information.
- To reduce the amount of space used on the 'z' drive ensure the information disclosed is only saved minimal times:
  If no review required – only keep the disclosure email which will contain the disclosed information (delete information saved to located information and request binder)
  If a review is required – only keep the track changed version sent back by the RC, once reviewed. Delete located information saved and the email sent to the RC for review (keep track changed version in the amendments folder and the final redacted version on the disclosure email that is sent and then delete the binder, hence, leaving just 2 copies saved in the log)
  If any deviation from the above is required - annotate the reason on the tracking log, i.e. One Drive disclosures

To support this, any reviews sent to SARs management team to review should be sent in word with track changes on.

21. Request Retention

As per NHS England Records Management Code of Practice[11] the retention period for Subject Access Requests is 3 years following the request being closed. If there has been an appeal the application is extended to 6 years following the appeal being completed.

Following review any deletion/ destruction will be captured on the Trusts disposal form and destroyed securely as per the Corporate Records Policy.

The Master Log will contain 10 years' worth of data for reporting and monitoring – it is acknowledged that for older applications the request folder will have been deleted and the only information available will be the minimal information contained on the Master Log.

22. Staff Privacy and Safety

To protect our staff all disclosures that include any reports that have been run for the purpose of a request must have ILR administration staffs name removed. This can be done by the SAR team prior to disclosure.

If there are any instances of harassment from requesters via email, telephone or in person or staff feel intimidated or scared they must:

- Inform their line manager.
- Complete an Eclipse incident form.

The situation can then be escalated to Stephen Laws the Trusts Local Security Management Specialist by Care Records management team

[11] NHSE Records Management CoP 2023 (england.nhs.uk)

Section B - Third Parties: Reviewer Role

This is only a brief outline of the considerations. For full guidance see 'Guidance on preparing information for disclosure under the GDPR'

Important Note: For NHS requests Third Party information can be automatically withheld so consultation is not required.

2.1. Is any 3rd party information contained in the files?

3rd parties may be individuals or organisations and includes information about/ provided by 3rd parties.

If the information is non contentious e.g. letters from other organisations, or NHS Trusts then it is your professional judgment as to whether this can be released.

2.2. Would the data subject know this information?

If they would know the information e.g., they were present at the meeting, there is little point withholding it.

2.3. Do we have consent to contact the 3rd parties?

We must check whether we have the authorisation of the data subject to contact any third parties mentioned within the information; if we do not have consent, we must not contact them. If we were to write to 3rd parties without consent, then this would release sensitive personal data about the person to the 3rd party and be a breach of Data Protection.

It will be evident from the application form whether consent has been given or not.

2.4. If we do have consent

- *For Record requests*: Inform Records staff who they need to write to and roughly what the information relates to. They will then contact the 3rd parties.

- *For non-Care Records requests*, e.g. Personnel: The person managing the request is responsible for contacting the 3rd parties. The Head of Information Governance / Head of Care Records can provide template letters for those.

2.5. Highlight the 3rd party information you are only happy to release if consent is provided by a 3rd party.

- If there is 3rd party information that you feel must be withheld regardless of consent ensure this is clear, e.g. use different colours to highlight the information.

- If there is more than one 3rd party, ensure it is clear which information relates to which person in case one consents and one doesn't.

2.6. Preparing the file

- *Care records request*: Care Records staff will release information as indicates by the relevant clinician so it must be clear to them what needs to be released, what doesn't and what is dependent on receiving consent.

- *Non care records requests*, e.g. Personnel: The person managing the request is responsible for contacting the 3rd parties. The Head of Information Governance / Head of Records can provide template letters for this.

Section C- Records/ appropriate review and writing to 3rd parties.

3.1. Write to the 3rd parties indicated by the reviewer.

Use letters SAR06 or SAR07 dependent on type of 3rd party e.g. individual or organisation?

3.2. Has the 3rd party replied?

If there is no response after 14 days assume that consent has not been provided and withhold the information.

If a response is received ensure it is clearly entered onto the request audit log and save the response in the 'Correspondence' folder for the request using format YYYYMMDD3rdPartyResponse (the date being the date you received the response)

- If this is in the form of an email save it in 'Outlook Message Format'

If a response has been received act as is appropriate to the response received, e.g. if consent has been provided the information can be released, if consent has been withheld the information should be withheld.

3.3. Prepare the information in line with the 3rd parties' response and disclose as appropriate.

Refer to Section A

Section D - What are the consequences of not following this guidance?

This guidance aims to help you comply with one of the obligations placed on the Trust by the GDPR. The consequences of failing to comply with the GDPR are serious. In the case of subject access requests:

4.1. Data subjects have the right to compensation in the event they are damaged by a contravention of the legislation, for example if we fail to supply them with the information they request (unless exemptions apply to that information), within the 30-day time limit and their interests suffer as a result.

4.2. Data subjects may complain to the Information Commissioner about any decision we make regarding the disclosure or non-disclosure of information. The Information Commissioner may serve an enforcement notice ordering us to release the information and for a breach can issue a monetary penalty notice of up to £17million or 4% of the annual turnover of the Trust.

Therefore, it is important that we disclose all the information that the data subject has requested but *only* that information which is liable for disclosure. We must do this within the 30-day time limit. In any dispute it is important that the Trust can demonstrate that normal practice was followed. This guidance represents normal practice.

Appendix 1: Definitions

Item	Definition
Subject Access Request (SAR)	Under the Data Protection Act, individuals can ask to see the information about themselves that is held on computer and in some paper records. If an individual wants to exercise this subject access right, they should write to the person or organisation that they believe is processing the data.
Personal Data	Personal data means information about a living individual who can be identified from that information and other information, which is in, or likely to come into, the data controller's possession.
Third Party	An individual/ organisation other than the Trust that has supplied/ volunteered information which relates to the Data Subject and is contained within their records.
Care Records (Supplementary Health Record - SHR)	Complete history of patient involvement with the Trust. This can comprise of paper Care Records as well as electronic data. The primary Care Record for the Trust is Rio with supplementary information being filed within the SHR. Historical information can be located in paper Care Records and via IFOS (Information From Other Systems)
Clinician	Member of staff with a medical background and currently working in a clinical area.
Corporate	Areas of the Trust that do not work with Service Users and perform central generic functions, e.g. Human Resources

Appendix 2: Template Letters

LETTER REF	DETAILS
SAR0	Egress Account Set Up
SAR1	Acknowledgment to requester (not a solicitor)
SAR1a	Acknowledgement to requester including application form [secure]
SAR1b	Acknowledgment no information held
SAR1c	Acknowledgement including ID guide
SAR2	Acknowledgement to Solicitor/Tribunal
SAR2a	Acknowledgement to police
SAR2b	Acknowledgement to solicitor
SAR3	Clinical Review with Staff Guidance and Consultation Reply Form
SAR3a	BHM Clinical Review
SAR3b	Police Clinical Review
SAR4	Valid consent required – representative applying for records
SAR5	Third Party – permission to contact needed from individual
SAR6	Third Party consultation with Reply Form – for individuals
SAR7	Third Party consultation with Reply Form – for organisations/ professionals
SAR8	Third Party chase letter
SAR9	Acknowledgment no information found Request Completed
SAR10	HMP inmate closure
SAR10a	Police Request Closed
SAR10b	Solicitor Request Closed
SAR11	Request collected and closed.

REMEMBER: Fill in the request Audit Log

SAR12	Request Cancelled
SAR13	Closure letter – application has been withdrawn, unable to disclose at this time
SAR13a	Unable to disclose – Law Enforcement
SAR14	Breach Advised
SAR15	Chase email for consent/W170
SAR16	Escalation of Breach to Clinical Director (CD)
SAR17	Staff reviews
SAR18	Forensic email notification to Trust staff from Associate Director of IG
SAR18a	Forensic Mail request to AD
SAR18b	Forensic Mail request to CEO
SAR19	ID Chase
SAR20	CCTV Acknowledgement request valid/ not valid
SAR21	Police Request Consent or WA170 required
NHS01	Acknowledgment
NHS02	No information held
NHS03	Request completed
A2HR0	Egress account set up
A2HR01	Acknowledgment with Application Form
A2HR02	Clinical Permission with Staff Guidance and Consultation Reply Form
A2HR03	Responsible Clinician Review Reminder
A2HR04	Reject application – to be completed by Team/Clinician copy to Care Records
A2HR05	Closure letter, enough information and identification provided
A2HR06	Closure letter – application has been withdrawn

A2HR07	ID Chaser Prior to Disclosure
A2HR08	Receipt of information – when being collected by hand
A2HR09	Acknowledgement – no information found

Appendix 3: Timeliness for Key Transactions

ILR Standards for Timeliness of Data Entry
(from January 2022)

Event	*Action &Enter onto Audit Log….*
Requests for personal data received by Information Requests (ILR) (bsmhft.informationrequests@nhs.net)	Logged within **2** working days of receipt
ILR Team to email sent to current/ most recent Clinician to query if review required	Within **3** working days
For requests where the Data Subject is a current In-patient ILR Team to email current Clinician to query if patient is well enough/ has capacity	Within **3** working days
Passed to SAR mailbox (bsmhft.SAR@nhs.net)	Within **2** working day once actionable
Pass to Digital Records Management (DRM) Team if paper records are required	Within **2** working day once actionable
Third Party Chase (if applicable)	Within **5** working days once advised by Clinician/ Line Manager following initial letter
1st Chase - Response from current/ most recent clinician if review required, Clinical Director is copied into email	On day **11** of the request if no response received
1st Chase - Clinician for review by SAR Team if applicable	Within **15** calendar days
2nd Chase - Clinician for review by SAR Team if applicable and to copy ILR Team	Within **20** calendar days
SAR Team to email CD and advise that request is due to breach	Within **20** calendar days
ILR Team to complete Eclipse Incident form as request has breached	On day **30** of the request
ILR Team to ID Chase (if applicable)	When ready to disclose if not already received. Advise requester of due date for receipt of ID if not received request will be closed

Key:

Key Transactions Completed by the Information Requests (ILR) Team
Key Transactions Completed by the Subject Access Requests (SAR) Team
Key Transactions Completed by the Digital Records Management (DRM) Team

REMEMBER: Fill in the request Audit Log

Appendix 4: ILR Flowchart

..\Current\20190228SARsProcessMap.vsd

Appendix 5: CCTV Flowchart

20240511CCTVFlowchart.docx

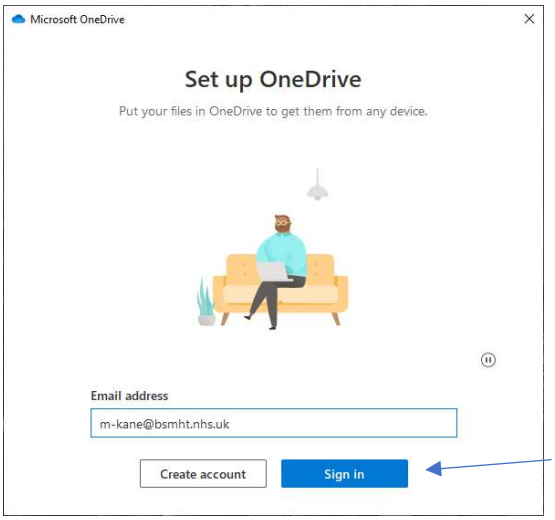
Appendix 6: Request Binder Process

Z:\Data Protection Requests\Procedural\Procedures\Current\20200907PreparingInformationForILR.pdf

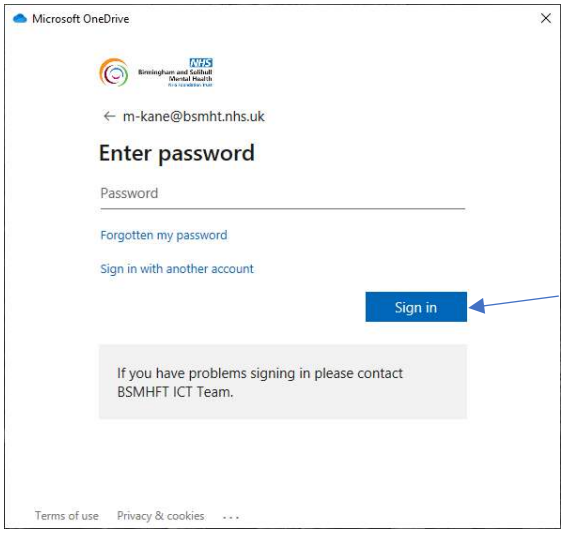
Appendix 7: Using OneDrive

Setting Up One Drive

- Click on Cloud symbol icon at bottom of desktop 
- Log on using your Bsmhft email leaving out the ‘f’ and not your nhs.net account as per the example below and click on ‘Sign In’.



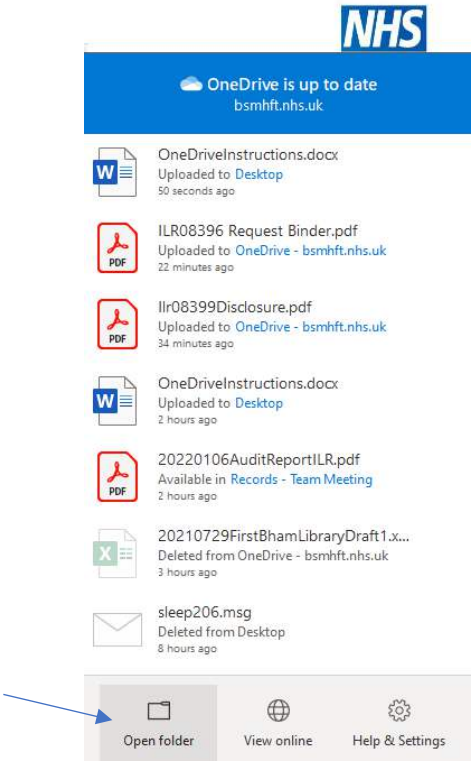
- You may not be asked for a password but if you are using the password, you log in to your PC with every day and then click on ‘Sign In’.



- Follow the prompts on screen, ie,
  - Next
  - Continue
  - Next
  - Later
  - Open my One Drive

- OneDrive will copy all the information that is on your Desktop and any information you have saved on your computer but not what you can access via Network e.g. Z Drive.

- To open OneDrive left click on the cloud icon at the bottom of your screen and then select ‘Open Folder’, from here you will see your documents you have saved on your computer, it is also in this view that you will be able to save documents direct into OneDrive



Send Disclosure via One Drive

- **Send** an initial email containing the amended disclosure letter advising you will be sending the disclosure via One Drive and asking them to ensure they check their *'junk mail'* in case the One Drive disclosure is there.

- **Add** the following to disclosure letter – '*Please be aware the disclosure will be sent shortly via One Drive. Please ensure you also check your junk mail.'*

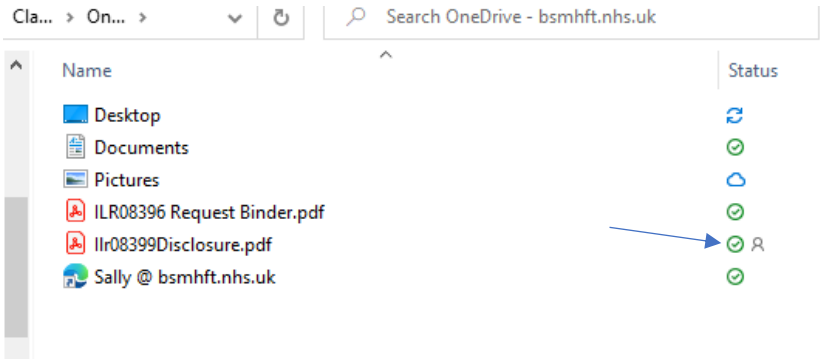
- **Copy** (Ctrl+C or Right Mouse Click) the Request Binder you are disclosing from the log (you will need to rename the binder so that you can easily identify the information you want to disclose, otherwise you risk sending the wrong information to the wrong requester i.e. ILR1234 Disclosure)

- **Paste** (Ctrl + V or Right Mouse Click) the copied binder into your OneDrive

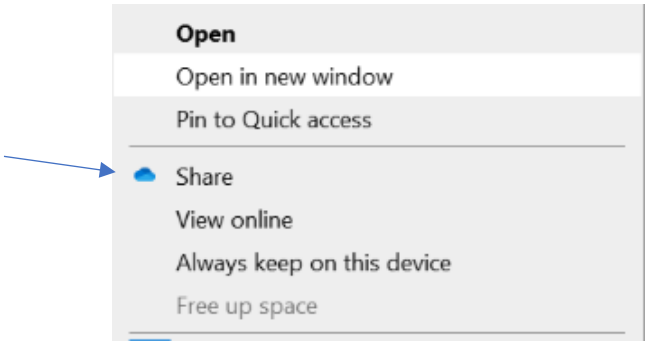
- If you don't use a binder, but have lots of documents to send i.e. CCTV requests, copy and past the folder the information is in, into OneDrive, once more remebering to rename the folder and remove any documents that are in there that you don't want disclosing such as the template Request Binders (as you have not used them) or any emails regarding the request. When ready **Copy** and **Paste** the folder into OneDrive. Please note if you have a lot of data it can take a few mintes until all the information is available to be shared in OneDrive. Please see points below

- You <u>do not</u> need to zip the documents/folder nor use a password

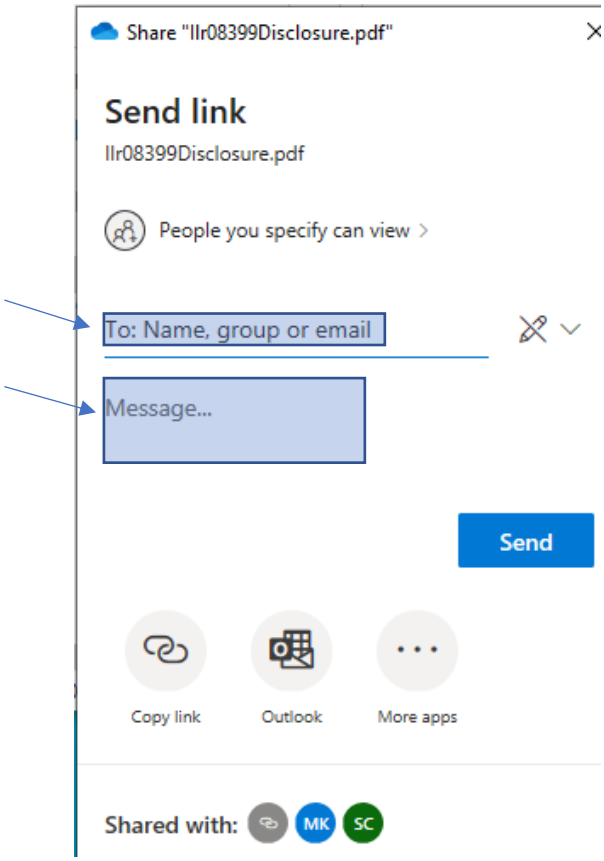
- Wait for the symbol under the status column at the end to present a green tick (this confirms it has now copied over) If you see a cloud or refresh symbol i.e. arrows making a circle this means the information is not ready. If you have copied a folder onto OneDrive you will need to open the folder to see the status of the documents to see if you are in a position to share.



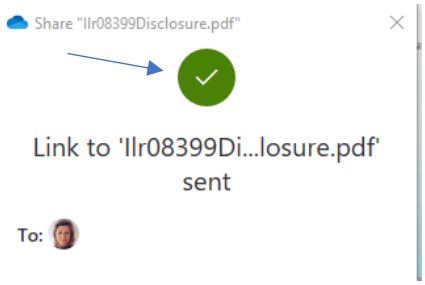
- When ready Right click on the information that you wish to send and click on 'Share'



- Once to selcet the option to share a further dialogue box will open.
- Type in email address of requester to send to (if you need to send to more than one recipient, type in a semicolan (;)



- Type in short message 500 characters maximum. Template letters cannot be used nor can subject line. Suggested message 'Please see link for the dislcoure of ILR1234. Please be advised that you will need to open/save/download within 5 working days as the link will be unavailable after this date'
- Press send (a tick will appear for confirmation it has sent)



- You will receive an email in your own inbox advising message sent. Save this to the ILR log

- You will receive a further email to your own inbox once the recipient has read the message. Also save this to the log

Housekeeping of your One Drive

- Please note that once you delete the disclosure from your OneDrive the recipient will no longer be able to access it

- You need to regularly delete disclosures from your OneDrive on a monthly basis, ie once a disclosure is 30 days old it should be deleted from your OneDrive account. This is a requirement of OneDrive, to free up space and allow OneDrive to work smoothly

- Housekeeping of your One Drive will form part of regular RMS's as reminder, to ensure OneDrive continues to perform correctly, reporting and for good record keeping

Appendix 8: Responsibility of Tasks

Information Legislation Request Function:

- Action requests sent to bsmhft.SAR@nhs.net email.
- Identify what information is required.
- Locate information.
- Clarify parameter of request with requester if unclear, ensuring the Information Request (ILR) team are copied in bsmhft.informationrequests@nhs.net
- Prepare information according to the Preparing Information for an ILR Disclosure document in the Request Binder, where appropriate
- Requests where disclosures need to be printed will be processed and printed by the SAR team (XXX,XXX,XXXX,XXX), by attending a Trust site do so. With the below options to send the printed disclosure:
    - Send in internal post to XXXX if it needs to go via DPO.
    - Send in internal post to Barberry to be sent recorded delivery.
    - Send recorded delivery yourself and claim charges back via expenses.
- Add closed date to individual log once disclosure has taken place.
- Add on hold date to individual log once disclosure is ready to send but are awaiting ID/consent before disclosure can be made.
- Advise ILR team when disclosure is ready but waiting for proof of identity that it needs to be placed on hold on the Masterlog.
- Chases to Clinician regarding completing review on set day count.
- Complete eclipse if sent without ID if it is required.
- Check ILRs for any updates on the log at day 15.
- Check ILRs for any updates on the log at day 20, prompting ILR team if there are no updates.
- Check ILR log on day 25 again for any updates and to avoid breaching.
- Save all correspondence sent and received i.e., emails, to Communications folder.
- Check ID/Consent headings on log has been updated reflecting any updates on the log.
- Requests for Tribunals send last 3 months of Progress notes unless otherwise stated, advising the Mental Health Legislation (MHL) team will forward most recent section papers only.
- Consolidated notes only cover Inpatient stays, therefore further progress notes may be required for any Outpatient history. Avoid downloading both as this causes repetition for the clinician during review, however in cases of Court Orders etc both consolidated notes and progress notes need to be included as data pulled through is not consistent in both.

Information Request (ILR) Managing team:

- Determine validity of request and log

- Send to SAR mailbox if valid request.
- Update log with ID/Consent when received.
- Enquire with clinician if a clinical review is required.
- When ILR team receive a response regarding review, they will copy in SAR team to ALL responses (whether a review is needed or not) and put on hold if we are still awaiting ID.
- Once ID is received, SAR team will only be advised if it is all that is required to complete the request (no point advising if we are still waiting for the RC).
- Complete eclipse for breaches including completing the questionnaire – NB. the questionnaire and eclipse needs to be updated and closed once ILR has been completed.
- Review requests where there is no response from Clinician – NB. XXXX, XXXX, XXXX, or XXXX to review for contentious information based on Risk Assessments completed, advising clinician if any identified and if still no response redact including any Safeguarding entries or entries marked ‘not for disclosure’. Corporate records request to be reviewed by XXXX.
- Once advised by SAR that the request is closed update Masterlog.

<u>Subject Access Request (SAR) Managing team.</u>

- Determine Information required with requester if unsure.
- Diarise all requests awaiting a response or ID.
- Escalate to Clinical Director on day 10 where no response is received from clinician.
- Send possible breach email/letter on day 20 and notify ILR if an eclipse is required.
- Move to closed log once closed.
- Notify ILR if no response is received from RC or CD and the request is disclosed.
- Notify ILR of closed requests in one email at the end of the working day.

Appendix 9: SAR Recall Process for Scanning Bureau

Introduction:
From the 5th of July 2021 the Records department commenced scanning in historical records for Subject Access Requests (SAR) following the process outlined below.

1. Information Requests (IR) will remain responsible for logging the request.
2. The request will be passed to the ILR and Pam Fishers (PF) mailbox once the application has met the legal threshold –

   NB: We are only looking to scan, currently, requests from Police, individuals, relatives, NHS/Health care provider, solicitors (not including Tribunals) under GDPR/Data Protection 18, Access to Health records and NHS Continuing Care so we are not currently including request for Tribunals, Coroners and Court orders unless paper is specifically requested, GMC etc. These will be processed later.

3. IR to highlight on the covering email to ILR and PF if the any paper records are required as part of the SAR and for what time period.
4. PF to triage all SAR notifications and prioritise any that require paper records to be recalled as part of the disclosure.
5. PF to review CRT and IM and recall all paper records including MHA files for the patient
   a. If there is a current file in use within the Trust this is to not to be requested – currently we are only scanning closed/ historical files.

      NB: If the file is required as part of the ILR then PF to liaise with Team to get record sent across.

   b. When the patient is discharged, or the file is no longer required, and it is returned to the Records Department the volume will be scanned at that time
   c. Should there be any previous ILRs in IM these are not to be recalled and scanned into OnBase as this will be a duplication of the information and could lead to confusion.
   d. Should there be any X-Rays, Videos or DVDs these are not to be recalled for scanning at this time.
6. PF to update CRT and IM with appropriate meta data.
7. PF to arrange for files that have been recalled from IM and are going to be scanned to be permanently removed from IM and update the Permanently Removal spreadsheet.
8. Any files that are required for a SAR are to be identified by PF by placing a sticky note on the front of the file
   a. PF to update ILR Audit Log to advise that the volumes have been received and that they are being sent to Northcroft for scanning.
9. PF to inform the Scanning Bureau that files are being sent to them which form part of a SAR disclosure and what volumes need to be prioritised – email to be sent to bsmhft.scanning.bureau@nhs.net

REMEMBER: Fill in the request Audit Log

10. Records to be tracked on CRT to 'Northcroft – Scanning Bureau'.
11. Records received at the Scanning Bureau and tracked in
12. Scanning Team to review records received and prioritise any volumes that are needed as part of a SAR – as per PF email.
    a. Where paper file is required and forms part of the disclosure urgently within 72 hours (this is to allow for any absences and any that have multiple and/or large files)
    b. Where there is a Court order, Coroner request etc. treat as an extraordinary request as a priority over all other work, ideally the same day dependant on number of files of course.
    c. where the paper copy is not required within 7 days
    d. Once scanned the Team to email PF to advise.
    e. PF to update ILR Audit log that volumes available on OnBase for processing.
13. If any files have any lose filing the Scanning Bureau to file this under the most appropriate section within the folder in readiness for scanning
14. Once volume is scanned the contents of the folder are to be place back into the folder they came out of and secured in the folder with an elastic band around the outside of the folder for transportation and storage
    a. There is no requirement for the contents of the folder to be threaded back onto the clips within the folders.
    b. Should the file be required after it has been scanned, identify the reason.
    c. If file required for filing arrange for the filing to be sent to Barberry for scanning preparation (NHS and Rio numbers, DOB etc.)
    d. If file is required to view, there are 2 options i) arrange for access for to On Base where it can be viewed; ii) send scanned file advising it will be in a post scanned state (a bundle as opposed to an organised file)
15. When all records have been scanned volumes to be tracked on CRT and returned to PF at 'Barberry – OnBase Storage'.
16. PF to receive and track in scanned files.
17. Current racking system to be divided into corporate and Clinical areas.
18. PF to store scanned Clinical files by month scanned and in alphabetical order of surname.
19. All scanned Personnel files are to be stored within the corporate area of the racking system in order of month scanned and alphabetical order of surname.

SSL Personnel files to be kept separate to Trust Personnel