Subject Access Request and Access to Health Records Procedure

NHS North Central London CCGs (Camden, Barnet, Enfield, Haringey and Islington)

Document revision history

Date	Version	Revision	Comment	Author
18 May 2018	4.0	Draft	Reflect re-branding and GDPR	IG Officer
October 2018	5.0	Final	Reflect procedural changes	IG Hub
March 2019	6.0	Revision	Localised for NHS North Central London CCGs	Dayo Adebari – Information Governance and FOI Manager – NCL CCGs

Document Approval

Date	Version	Revision	Role of approver	Approver
23/05/2018	4.0		Director of Governance	Finance and Audit Group
16/10/18	6.0	GDPR / DPA 2018 Compliance		Information Governance Group

Contents

..... 1

Definitions 5

Introduction 6

1. Purpose 6

2. Scope 6

3. Duties and responsibilities 7

4. Administration of requests 8

Administration of Requests – NEL SARs 8

Administration of Requests – Customer SARs 9

Acknowledgement of the request 9

Confirmation of identity 9

Clarification of scope 10

Request forwarded to relevant service for collation 10

Issues engaged and exemptions 11

Third Party Information 12

Redaction 13

Preparation to dispatch information 13

5. Subject access requests 13

Recognising and Receiving Requests 13

Minimum Requirements for a valid request 14

Retention schedules 14

Requests relating to children 14

Requests on behalf of a third party 14

Requests to view original health records 15

Appropriate Health Professional for Health Record requests 15

Fees 15

Subject Access Request – Staff Records 15

Freedom of Information and Other Requests 15

Request to Access Records of the Deceased 16

6. Non-statutory releases of personal information 16

7. Requesting amendments, corrections or deletions 17

8. Monitoring Compliance 17

9. Review and version control 17

10. Latest version 17

11. References 18

12. Implementation plan 18

13. Equality & Equity Impact Assessment Checklist 18

14. Data Protection Impact Assessment 19

15. Complaints 20

Appendix A - Requests for access to information 21

Under the Access to Health Records Act 1990, Data Protection Act 2018 and General Data Protection Regulation – as referenced in the DPA 2018 21

Consent form for the review and release of records containing personal data 21

What you need to complete: 21

Section 1 - Your Details 21

Section 2 – Your Information 21

Please indicate what is being applied for: 22

Please indicate the Borough or County to which your request relates 22

Date and type of records 22

Section 3 – Your Identity 23

Section 3.1 – Requesting a Child's Information 23

Section 3.2 – Applying for access for an authorised representative 23

Section 4 – Your Authorisation 24

Section 5 – Return Details 24

Section A – Requesting Health Records of the deceased 25

Details of the deceased 25

Details of the deceased's GP 25

Any other details you may feel are relevant and will help us locate the information 26

Retention of Personal Information 26

Appendix B – Standard letter text for acknowledging requests and/or requesting more information . 28

Appendix C – Standard letter text enclosing information 30

APPENDIX D – PROCESS OVERVIEW 31

Definitions

- **Disclosure** – disclosure of personal information or data by transmission, dissemination or otherwise making available.
- **Exemption** – information withheld from release due to an exemption in the General Data Protection Regulations or Data Protection Act 2018
- **Controller -** A controller determines the purposes and means of processing personal data**.**
- **Processor** - A processor is responsible for processing personal data on behalf of a controller.
- **Health Professional (HP**) – Registered, Qualified and appropriate individual as defined by Section 204 Data Protection Act 2018. The HP can make judgement on the serious harm test, where they have had with the most recent responsibility for the diagnosis, care or treatment of the patient, if more than one clinician the most suitable to provide an opinion or who has the necessary experience (if the most recent is not available). The HP can also facilitate the viewing of a record and can comment upon the content, especially valuable for the explanation of medical terms.
- **Lay Administrator**- an administrator or non-clinician who will support viewing access to a record in order to (i) protect the integrity of the record and (ii) assist the requestor. However, the Lay Administrator can provide no comments or analysis of the content.
- **Personal Data** – is any information relating to an identified or identifiable living individual.
- **Identifiable living individual -** means a living individual who can be identified, directly or indirectly, through:

  a. an identifier such as a name, an identification number, location data or an online identifier, or;
  b. one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
- **Data subject** - The identified or identifiable living individual to whom personal data relates.

- **Patient/Personal Confidential Data (PCD)** – personal (or Patient) Identifiable Data, Information that can identify an individual.
- **Public Interest -** a process for deciding whether information about individuals should be disclosed outside of statutory requirements. The judgement must assess the duty and expectation of confidentiality against the public interest in accountability, transparency and scrutiny of public duties.
- **Special Category Data –** this is a list of types of information that are classed in accordance of the GDPR as sensitive and require further justification for processing data.
- **Serious Crime –** a serious crime is defined by the General Medical Council (GMC) as "a crime that puts someone at risk of death or serious harm and would usually be crimes against the person, such as abuse to Children"- *GMC guidance Confidentiality: Protecting and Providing Information paragraph 37*.
- **Serious Harm-** There are two definitions of serious harm:
  - Individual: The Serious Harm test is applied where 'the data would be likely to cause serious harm to the physical or mental health of the data subject or another individual' Section 2(2), Part 2, Schedule 3, Data Protection Act 2018
  - . or
  - Serious: harm to the security of the state or public order and crimes that involve substantial financial gain or loss will also generally fall within this category – *DH: Confidentiality NHS Code of Practice page 35 figure 7*.
- **Third party Information** – Information contained within a record that relates to another individual, such as a sibling.

Introduction

This procedure details the approach to managing Subject Access Requests (SARs) made under the Data Protection Act 2018 (DPA 2018) and General Data Protection Regulation (GDPR) as referenced in the DPA 2018[1], and Access to Health Records Act 1990 (AtHRA). This includes requests for Health Records, staff records and any other information held about individuals. This process can also be triggered by requests under the Freedom of Information Act 2000 (FOI), which engage exemption 40, personal information relating to a third party access request.

1. Purpose

This procedure provides North Central London Clinical Commissioning Groups (NCL CCGs) with an overarching framework for the management of requests for personal information for living individuals under GDPR/DPA (2018) and for deceased individuals under Access to Health Record Act (AtHRA). It defines a process for achieving legislative requirements and ensuring effective and consistent management of requests.

Where the NEL Information Governance function offers a Subject Access Request service, this procedure also provides the framework for handling requests for customers. This service is managed by the Information Governance Function of NEL.

NEL acknowledges the importance of openness with employees, patients, customers and clients and in co-operating with them for requests and applications to access to records or information containing their personal data.

Most elements of this guidance and procedure will be the same for both NEL and customers. Where a separate process or consideration might occur, that section will clearly identify whether it applies to NEL or customer. Unless otherwise stated, all sections should be read as applying to both entities.

2. Scope

This procedure relates to all personal records held by NHS North Central London CCGs and where NEL provides a SARs service, to Customer held records.

All NHS North Central London CCGs staff must adhere to this procedure and managers must ensure that all those working on behalf of the CCGs are aware of this document.

It is noted that GDPR/DPA (2018) covers information held across all formats including, but not limited to electronic systems and paper records. This procedure covers applications to view personal information under the GDPR/DPA (2018), FOI and AtHRA.

An individual can make an application for access regarding his or her personal data to NEL or to a Customer by any of the following:

- Personally;
- A person authorised by the individual in writing to make an application on an individual's behalf;
- A person having parental or guardian responsibility for the individual where he/she is a child;
- A child under the age of 16 who is deemed mature and able to take decisions about treatment. The ICO advise only children aged 13 or over are able provide their own consent;
- A person appointed by the court to manage who is deemed competent;

[1] Documented as the Data Protection Legislation from this point forward.

- A person appointed by the courts to manage the affairs of mentally incapacitated adults in order to fulfil their function to seek access;
- Where the individual has died, the personal representative (Executor of the Will) and any person who may have a claim arising out of the individuals death;
- Solicitor acting on behalf of an individual.

This Subject Access Request Procedure contains a number of safeguards and exceptions that are designed to ensure the following:

- Controllers must seek to verify identity of the data subject where there are 'reasonable doubts.'
- That individuals have a right to access their information, although there are exceptional reasons and tightly defined circumstances where this can be denied, i.e. on grounds of potential harm to the physical or mental health of the patient That unless the source of the data is a Health Care Professional engaged in the direct care of the individual, that the identity of an individual who provided/recorded information should not be disclosed, nor should the identity of any other person/s referred to in the record(s) of the individual requesting access, unless explicit consent has been given.

3. Duties and responsibilities

Accountable Officer – as Accountable Officer is responsible for ensuring that Subject Access Requests are handled in accordance with the law.

Data Protection Officer – advising on how compliance will be achieved and demonstrating Subject Access Requests are handled in accordance with the law.

Director of Corporate Services - has overall responsibility for Information Governance. They are responsible for the management of the organisation and for ensuring the implementation of appropriate mechanisms to support service delivery and continuity. Information Governance is key to this as it ensures appropriate, accurate information is available as required.

Senior Information Risk Owner (SIRO) - is appointed by the Internal Assurance Group and is accountable to the Senior Leadership Team for the appropriate management of risk associated with the organisation's use and holding of information.

Caldicott Guardian – as responsible executive for the confidentiality and data protection assurance agenda, the Caldicott Guardian is responsible for ensuring that the systems in place meet requirements and that staff are adequately trained and aware of their responsibilities. The Caldicott Guardian sign off the final copy the request.

Information Governance Group (IGG) - the IGG have Data Protection and Confidentiality within their remit and support this procedure by monitoring the performance of service areas providing the response, providing an overview of the impact on the organisation and reviewing updates from the IG Manager and IG Team.

NEL IG Team – CSU SARs - The IG Manager and team are responsible for providing the SARs service for the CSU, as well as guidance and support made under the GDPR/DPA (2018). They must also ensure that an annual report is produced; they are responsible for maintaining, reviewing and improving this procedure.

NEL IG Team – Customer SARs - Where customer SARs are concerned, the IG Manager and team are responsible for providing the SARs service as well as providing guidance and support made under the GDPR/DPA (2018).

All staff - are expected to recognise and action Subject Access Requests within one working day. These should be highlighted to the line manager and forwarded to the IG Team immediately.

Email: NELCSU.Information-Governance@nhs.net (From nhs.net accounts only)

By Post to Information Governance Team, NEL, 1 Lower Marsh, London, SE1 7NT
- Where practicable, translation services to assist can be accessed in the usual manner, for other questions contact the Information Governance Team.

Failure to pass requests on or ensure they are actioned may be a breach of contract in addition to a breach of the GDPR/DPA (2018) and can be subject to disciplinary action.

It is the responsibility of all staff for abiding by this procedure and in discharging their duties in accordance with law, ensuring that the confidentiality and security of information in all formats is maintained and that any disclosure is appropriate and provided to the correct contact point. They are supported in this by the procedures, best practice guidance and the Information Governance Framework.

Non-compliance - Failure to comply with the standards and appropriate governance of information as detailed in this protocol can result in disciplinary action. All staff are reminded that this procedure covers several aspects of legal compliance that as individual they are responsible for.

Failure to maintain these standards can result in criminal proceedings against the individual or organisation.

4. Administration of requests

Administration of Requests – NEL SARs

The IG Hub Team will hold and maintain a central spreadsheet with a minimum data set for recording the Subject Access Request which must contain the following:

- **Unique ID**
- **Status** – reflects the current status of the request Open, Closed, Seeking Clarification
- **Date received** – the date the request was received
- **Date ID Checks Completed** – date the IG team receives sufficient and appropriate confirmation of the data subject's and where different, the requestors identity
- **Statutory Deadlines –** One calendar month commencing from the date ID is confirmed
- **NHS Deadline** – 20 calendar days from the date received for records updated in the last 40 calendar days, and one month for those records which have not been updated in past 40 calendar days
- **Extension –** If a request is either complex or numerous, any extension is recorded along with the new deadline and when the data subject was notified
- **Completion Date** – the date the response is sent to the requestor
- **Notes** – Covering any actions updates and exemptions under consideration.

The spread sheet and all documents related to the request will be stored on the shared IG Team SharePoint Hub Library with access restricted only to those who have authority to manage such requests.

Additional data will be recorded as required for the monitoring and management function. The spread sheet will cover the current financial year and will be archived as appropriate – see Retention Periods below.

Within the confidential location an individual folder will be created for each request and all relevant documentation, including correspondence with on-going business value (for example, concerns over serious harm or distress or the presence of third party information).

Please also see the flow chart and forms in the appendices.

Administration of Requests – Customer SARs

The IG Hub Team will hold and maintain a central spread sheet for each customer where a service is provided.

The minimum data set for recording the Subject Access Request must contain:

- **Unique ID**
- **Status** – reflects the current status of the request Open, Closed, Seeking Clarification
- **Date received with the Customer** – the date the request was received
- **Date received at the CSU IG Team** – the date the request was received by the IG Hub
- **Date ID Checks Completed** – date the IG team receives sufficient and appropriate confirmation of the data subject's and where different, the requestors identity
- **Statutory Deadlines –** One calendar month commencing from the date ID is confirmed
- **NHS Deadline** – 20 calendar days from the date received for records updated in the last 40 calendar days, and one month for those records which have not been updated in past 40 calendar days.
- **Customer contact** – the member of customer staff (and their contact details) liaising with the IG Team.
- **Date client advised to proceed with SAR**
- **Date information received from customer contact**
- **Extension –** If a request is either complex or numerous, any extension is recorded along with the new deadline and when the data subject was notified.
- **Completion Date** – the date the response is sent to the requestor
- **Notes** – Covering any actions updates and exemptions under consideration.

The spread sheet and all related documents to the request will be stored in a confidential folder in the Information Governance SharePoint Hub Library with access restricted only to those who have authority to manage such requests.

Additional data will be recorded as required for the monitoring and management function. The spread sheet will cover the current financial year and will be archived as appropriate – see Retention Periods below.

Within the confidential location an individual folder will be created for each request and all relevant documentation, including correspondence with on-going business value (for example, concerns over serious harm or distress or the presence of third party information).

Please also see the protocol in the appendices

Acknowledgement of the request

Any necessary acknowledgement is dispatched by the information governance Hub Team once a log is made of the request. If the information is not available on the request form, the information governance Hub team will determine which service is likely to hold records or whether the record is held by the shared service facility.

Confirmation of identity

If there are reasonable doubts, the identity of the individual may need to be confirmed with the following documentation, which is also listed on the form: The IG Hub team will request and review all identity documents received and check that they are valid. The legal timeframe for a SAR only commences once identity has been established.

If an adult, the individual must provide good legible photocopies of one type of identification from this list:

- Passport, driving licence,

- Government Issue photo identification,
- NHS card, tenancy agreement, credit or bank card, birth certificate.

And one additional proof of address from the following list:

- Rent card or book,
- Benefit book,
- Council tax bill,
- Utility bill within last 3 months,
- Credit or bank card statement within the last 3 months,
- Letter from a government department or local authority.
- If the individual is a child, we require a copy of their birth certificate only.

Clarification of scope

Acting in the interests of the data subject, the IG Hub team will liaise with the requestor to clarify the scope of the request. This may include clarification of which team / department / service is likely to hold the record and may include discussion on timeframes and nature of records requested to assist the requestor in accessing the records they need or wish to locate.

Particularly where copies of emails are requested, clarification of scope may include discussion about limiting time periods and correspondence between named individuals for example. Requests which ask for 'all data', especially where emails are requested can generate significant volumes of material in response to the request. Requests for 'all data' may be categorised as manifestly unfounded, excessive or complex resulting in the request being denied, charged for or extended by two months (to a three month maximum response time). Clarification of scope has the benefit of being able to reduce the risk of this happening.

Request forwarded to relevant service for collation

After the request has been logged, acknowledged and identity and scope confirmed, the details of the request are forwarded to the relevant service or customer to collate a copy of the electronic records and any paper records that have been requested. Following collation, this must be reviewed by an appropriate member of staff within the internal service or customer for the following issues:

- Any terminology or abbreviations that might require further explanation
- Was any information disclosed to us from another Controller, is it clear whether this information is intended to be included in the record? Should the other Controller be contacted to review?
- Could the information released cause serious harm to the physical or mental health or condition of the individual, or any other person?
- Access would disclose information relating to or provided by a third person who has not consented to that disclosure unless:
    - The third party is a health professional who has compiled or contributed to the health records or who has been involved in the care of the patient.
    - The third party, who is not a health professional, gives their consent to the disclosure of that information.

A copy of all relevant information together with any concerns must be passed to the relevant Clinical Lead (usually the Caldicott Guardian or an appointed and trained clinical lead acting under the direction of the Caldicott Guardian) for review where the request is for patient data and the SIRO for employment data and prepared for release within the statutory timescales. Original records **must never** to be dispatched to the requestor.

Issues engaged and exemptions

Where issues are identified, the NEL Information Governance Team will discuss and advise the identified lead for the request whether some information can be released, whether it should be redacted or whether the release should be refused.

- Exemptions that would prohibit disclosure include: Article 23 GDPR allows organisation to place exemptions on the rights of data subjects in certain circumstances:
    a. National Security;
    b. Defence;
    c. Public Security;
    d. The prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the prevention of threats to public security;
    e. Other important objectives of general public interest, for example monetary, budgetary and taxation matters, public health, and social security;
    f. The protection of judicial independence and judicial proceedings;
    g. The prevention, investigation, detection, and prosecution of breaches of professional ethics;
    h. Certain monitoring, inspection, and regulatory functions;
    i. The protection of the data subject or the rights and freedoms of others;
    j. The enforcement of civil law claims;

Schedule 2 & 3 DPA (2018) provides further relevant exemptions:

- Regulatory functions relating the health service: if Information requested is processed in accordance with Section 14 NHS Redress Act 2006 and/or section 113(1) or (2) or section 114(1) or (3) of the Health and Social Care (Community Health and Standards) Act 2003, an exemption will apply where this would likely 'prejudice the proper discharge of the function';

- Legal Professional Privilege: Personal data is exempt where 'a claim to legal professional privilege…. could be maintained in legal proceedings';

- Management Forecasts & Planning: Information can be excluded where it is '…likely to prejudice the conduct of the business or activity concerned';

- Negotiations: Information that records the intentions of the controller in any negotiations with the data subject can be excluded in so far that the information 'would be likely to prejudice the conduct of the business or activity concerned';

- Confidential References: References can be excluded if given in confidence for actual or prospective:
  (a) education, training or employment;
  (b) Placement as a volunteer;
  (c) Appointment to any office;
  (d) Provision of any service;
- Research and Statistics: personal data for archiving purposes in the public interest, scientific or historical or research purposes and statistical purposes can be excluded where, as confirmed in Section 19 DPA (2018), '…is likely to cause substantial damage or substantial distress to a data subject.' Exclusion must also occur where processing is completed for 'the purposes of measures or decisions with respect to a particular data subject, unless the purposes for which the processing is necessary include the purposes of approved medical research';
- Data Processed by a Court: Personal data is exempt if:

(a) 'it is processed by a court';
(b) 'It consists of information supplied in a report or other evidence given to the court in the course of proceedings…'
(c) 'In accordance with those rules, the data may be withheld by the court in whole or in part from the data subject';

- Protection of the Rights of Others: If any data identifies a third party, there is no obligation for a controller to disclose this data to the data subject. The Controller may still refuse to disclose information where consent has been provided or it is reasonable to disclose without consent;

- Data Subject's Expectations and Wishes: If a data subject is either under 18 and the request is made by an individual who has parental responsibility or the data subject is incapable of managing his or her own affairs and a power of attorney is appointed, information can still be withheld if:
    a. Information was provided by the data subject in the expectation that it would not be disclosed to the person making the request;
    b. Information was obtained as a result of any examination or investigation to which the data subject consented in the expectation that the information would not be so disclosed;
    c. The data subject has expressly indicated that information should not be so disclosed;

- Serious Harm: If an appropriate health professional's opinion is that serious harm would be caused, the data can be withheld. DPA (2018) defines serious harm as '… likely to cause serious harm to the physical or mental health of the data subject or another individual'. Any opinion must have been provided six months prior or during the time of the request. It may be necessary, even if an opinion was sought beforehand, to re-consult with an appropriate health professional to ensure that any exemption is still relevant;

- Child Abuse Data: If a data subject is either under 18 and the request is made my an individual who has parental responsibility or data subject is incapable of managing his or her own affairs and a power of attorney is appointed, child abuse data can be withheld if it would not be in the best interests of the data subject;

Other exemptions within DPA (2018) and subsequent Statutory Instruments will be considered by the Information Governance Team.

Third Party Information

Where third party information is contained within information subject disclosure, but consent cannot be obtained, the controller can make a judgement on whether it would be reasonable to disclose the information without a third party's consent. This judgement must be recorded and should consider:

- Initially consider whether there is any information that would already be provided to the Data Subject or is the Data Subject already or likely to be their possession
- The type of information that would be disclosed;
- Any duty of confidentiality owed to the other individual;
- Any steps taken by the controller with a view to seeking the consent of the other individual;
- Whether the other individual is capable of giving consent;
- Regard for the relevance of the information and how personal, intrusive or extensive it may be;
- Any express refusal of consent by the other individual.
- If the Caldicott Guardian was consulted

These issues are handled on a case by case basis and guidance will be sought on what is reasonable within the circumstances. It is recommended that in areas of doubt, consent from the third party should be sought.

Redaction

Following review and consideration of the collated response to the request by the service lead and the Caldicott Guardian, any data which is agreed should be removed needs to be redacted from the data prior to release. This is normally undertaken by the service lead.

There is only one recommended method for permanent redaction of data and this is to use Adobe Acrobat XI (eleven) Pro or later versions. This software easily and permanently redacts data. This will require all documents to be in pdf format.

Following redaction, pdf copies of the response to the request should be filed with the IG Hub team for secure storage.

Important

Original records must never be redacted. Only copies of the original must be redacted.

Redaction is frequently not necessary and often where it is needed its use is often sparse.

Preparation to dispatch information

The copy of the information to be disclosed will include details of their right of complaint to the Information Commissioner's Office. Where information was provided by another Controller and not considered within the scope of the request the data subject must be informed of the existence of this information and should be advised to contact the relevant controller unless exemptions apply (for example, investigation of crime or taxation).

Where the request does not specify a format in which the information should be provided, GDPR specifies that where requests are received electronically, the response should be provided in the same way.

If providing information in hard copy, copies can be collected from an appropriate site, which should be confirmed before the records are collected, or should be dispatched by recorded delivery in appropriate packaging to the contents. The envelope will be addressed as Private and Confidential with a return address on the reverse.

A copy will be kept of the record delivery details. Due reference must be made to Safe Haven Procedures as detailed in the relevant policy and procedure.

The identity must be checked of anyone picking up copies and a signature must be obtained and a receipt issued.

5. Subject access requests

It is not expected that NEL or its customers will receive a significant number of Subject Access Requests for Health Records due to services being provided. Where necessary an appropriate Health Professional will be identified or guidance sought from the Caldicott Guardian, or the equivalent at the customer organisation.

Recognising and Receiving Requests

Requests for access to information held about individuals are made under the terms of GDPR/DPA (2018). The request can be made verbally or in writing. Requests must be made by individuals or a duly authorised representative acting on their behalf.

The form Request for Access to Information, under GDPR/DPA (2018), should be made available to members of the public, in order to assist members of the public in making these requests for any

information held about them- See Appendix A. The form is not mandatory but is there to help requestors frame their request. Any request in writing forms a valid request where authority is present.

The form advises the requestor on the application of the various options and requirements to provide relevant identification in order to facilitate the request.

This form can also be completed by employees or those wishing to access other information held about them and will be made available on the NEL intranet.

Minimum Requirements for a valid request

In order for the request to be processed, the following is required:

- Sufficient information to identify the individual such as name, contact details, date of birth
- The applicant is also advised to provide additional information or, in the case of a change of name or address, any information that might assist the location of the file.
- The individual is not required to disclose or provide any reasons for requesting access.

The form also obtains their consent to produce copies of the record in order to process their request.

The individual will need to confirm their identity where the Controller has reasonable doubts. Where an authorised representative is making the request, both consent and authorisation of identity must be presented as part of the request. However, if a Solicitor or Legal Representative makes a request on behalf of a data subject, the request can be accepted without any further checks.

If the form is not completed or unclear, NEL will contact the applicant to request clarification however; this will not pause the time period for completion.

Retention schedules

Retention Schedules from the Records Management Code of Practice for Health and Social Care 2016 will be applied to all requests 3 years after the last recorded action and then will be destroyed under confidential conditions. Where the response to a request has resulted in an appeal, these requests will be kept for 6 years after the last recorded action and then will be destroyed under confidential conditions.

Requests relating to children

Where requests relate to information held about a child it is important to determine whether there is a legal right to access those records. It is important to consider:

- The duty of confidentiality owed to the child;
- Whether disclosure could result in serious harm to the individual or any other person; and
- Those children under the age of 13 who have capacity to take decisions about treatment to which they are entitled to.

Where health records are concerned, good clinical practice dictates that children should be encouraged to involve parents or other legal guardians in their healthcare.

Requests on behalf of a third party

Requests made on behalf of someone else, if not from the individual's legal representative, will require identification for both parties, in addition to the relevant consent and or proof of parental responsibility where applicable.

The proof of identification is to be shown to a member staff, if the records are to be collected from site or should be provided by post if records are to be sent via post. A record should be made of what identification was seen and by whom. A receipt can be issued if it is deemed appropriate.

Requests to view original health records

Patients may request to view their original health records through the Subject Access Request procedure. NEL and its customers are under no statutory duty, with few exceptions, to provide such access and can do so only in agreement with the data subject. Requests to view records will be dealt with on a case-by-case basis subject to restrictions on resources. In order to facilitate the viewing of records, the CSU or customer may impose a pre-condition to ensure the viewing of records will effectively deliver a review of records and answer any concerns. This can include the requirement to specify concerns or a range of records to review.

Access to records must be supervised either by an appropriate Health Care Professional, or a Lay Administrator usually provided by the Information Governance Team.

The Lay Administrator cannot advise or comment on the content of the record. The data subject will be advised of these conditions in writing before the appointment to view.

Appropriate Health Professional for Health Record requests

Section 17, Part 3, Schedule 2 DPA (2018) confirms it is reasonable for a controller to disclose information to a data subject without the consent of a Health Professional (Health Data Test) where:

- The information in question is contained in a health record, and;
- The other individual is a health professional who has compiled or contributed to the health record or who, in his or her capacity as a health professional, has been involved in the diagnosis, care or treatment of the data subject.

Fees

There is no standing right to charge fees under Data Protection legislation.

However, where the legislation states that a request is deemed to be manifestly unfounded or excessive under GDPR, NEL and its' customers reserve the right to charge an appropriate fee in order to recoup the costs entailed as compliant with GDPR.

Subject Access Request – Staff Records

Under GDPR/DPA (2018), staff have a right to request all the information their employer holds on them. This process is administered in the same way as that outlined under section 5 with the variations being as follows:

- The information is reviewed by an administrator nominated by the Human Resources Department who will consider any exemptions, redactions and third party information;
- Identity checks and details for the request are the same as in the procedure above. However, it is accepted that if an employee is known to the organisation, this may provide sufficient proof of identity;
- The employee can request to view original records but subject to the ability to resource and assist, and may have pre-conditions. The judgement of the Human Resources will be sought in assisting these requests.

In addition requests under GDPR/DPA (2018) for employees can include access to any emails retained by the organisation that refers to them. This must be considered if requested for disclosure with particular attention paid to reported opinions of third parties.

Freedom of Information and Other Requests

Requests made for information held about individuals that does not fall into the above categories must also be considered. The request has to come from the subject of the request or a duly appointed representative to which the subject has provided consent to disclose the information. These requests can be received under FOI.

The above procedure is followed in all respects. The only deviation being the nomination of an appropriate administrator to review the file for third party information, and other information subject to exemption listed above.

Request to Access Records of the Deceased

Under the terms of the AtHRA, requests can be made to access the health records of a deceased person. Under the terms of the Act the following have a right to request access:

- The patient's personal representative, this is the executor or administrator of the deceased person's estate.
- Any person with a claim arising out of the patient's death.

The right afforded to those with a claim on the estate is limited to information relevant to that claim and requests should be assessed on that basis. It may be necessary to request more details of legal proof of this claim. Ultimately, the Information Governance Team will determine whether this claim is justified and may advise seeking legal advice.

The personal representative has an unqualified right of access to a deceased patient's record and need give no reason for applying for access to a record.

In all circumstances, the identity of the requester and any relationship to the deceased must be proved. The serious harm and third party confidentiality rules will still apply. It may be necessary to refer more sensitive cases to the Caldicott Guardian where appropriate.

See the flow chart at appendix D.

6. Non-statutory releases of personal information

There are several circumstances where information may be released outside of the context of statutory requirements. In these situations it is vital to consider the decision making and document the reasons. Current judgements of courts indicate that the duty of confidentiality, within a medical setting, extends after death. The judgement will need to be based on:

- duties and expectations of confidentiality
- consent or express wishes of any of the individuals involved
- importance of the providing a confidential health service
- the legitimacy and proportionality of the request

Disclosures in such circumstances must be considered on a case by case basis and:

- considered to be in the public interest to release the records
- proportionate in meeting the requirements of the request
- that the request is legitimate and offers benefit, for example to surviving relatives, and would not cause serious harm to the mental or physical health of any individual

In such situations staff are asked to discuss the disclosure with the NEL Information Governance Team, who will advise whether the Caldicott Guardian or legal advice should be sought. In all circumstances the requester will need to provide proof of identity and of the legitimacy of their request, and their relationship with the individual.

7. Requesting amendments, corrections or deletions

Those with information held by NEL or Customers may request amendments, corrections or deletions as virtue of Article 16 GDPR. Any such requests should be discussed with the relevant line manager and the NEL Information Governance Team.

8. Monitoring Compliance

Compliance with all aspects of information governance will be undertaken as part of the information governance work plan or at the direction of the Information Governance Steering Group and the Senior Information Risk Owner (SIRO) or Caldicott Guardian.

Document Audit and Monitoring Table	
Monitoring requirements **"What in this document do we have to monitor"**	We will ensure that staff are aware of the Procedure, the constituent aspects of the information governance framework, and abide by legal, technical and mandatory IG requirements Performance in the Information Governance Toolkit and the completion of a Data Flow Mapping exercise
Monitoring Method	Data Security and Protection Toolkit annual assessment
Monitoring prepared by	Information Governance Manager
Monitoring presented to	Information Governance Group (IGG)
Frequency of presentation	Annual independent audit, submissions in line with Department of Health Guidance

9. Review and version control

Review will take place every three years until rescinded or superseded.

10. Latest version

The audience of this document should be aware that a physical copy may not be the latest version, the latest version, which supersedes all previous versions, is available at the location indicated in the document control section of this document. Those to whom this procedure applies are responsible for

familiarising themselves periodically with the latest version and for complying with procedure requirements at all times.

11. References

Data Protection Legislation - rights for living Individuals to access their own records the right can also be exercised by an authorised representative on the individual's behalf.

Access to Health Act 1990 - the right to access deceased patient's records by specified persons.

Access to Medical Reports Act 1988 – right for individuals to have access to reports, relating to themselves, provided by Medical Practitioners for employment or insurance purposes.

Freedom of Information Act 2000 - access to information held by Public authorities

12. Implementation plan

The updated Procedure, once approved by the NEL's Information Governance Steering Group will be shared with all staff through the all staff email, updated on the intranet, and shared with the Board. A team briefing will be provided to support this dissemination.

Awareness of the policy will be checked through a staff survey and spot checks on at least an annual basis. Customers will be responsible for ensuring availability of this policy to their staff and ongoing staff communications to increase awareness of this and other policies.

13. Equality & Equity Impact Assessment Checklist

This is a checklist to ensure relevant equality and equity aspects of proposals, policy or guidance have been addressed either in the main body of the document or in a separate equality & equity impact assessment (EEIA)/ equality analysis. It is not a substitute for EEIA/ equality analysis which is normally required unless it can be shown that a proposal has no capacity to influence equality. The checklist is to enable the policy lead and the relevant committee to see whether the EEIA has covered the ground and to give assurance that the proposals will not only be legal but also fair and equitable and lead to reduced health inequality.

	Challenge questions	Yes/No/ DK/NA	Comments
1.	Does the document set out the **health care needs** of the groups intended to benefit from the proposal, including any differences in need in terms of the legally protected or other characteristics (such as socioeconomic position)	N/A	
2.	Does the document set out any known existing inequality in **access**, **quality**, **experience** and **outcome of care** for populations relevant to the	N/A	

	proposal (i.e. as defined in 1. and in relation to the existing health or care service)?		
3.	Are there any particular **public concerns** about equality about the policy area than need to be addressed?	N/A	
4.	Has the policy described any **gaps in knowledge** about 1 -3, and any action taken to fill gaps (or recommendations for action)		
5.	Does the document set out **risks to equity** of access, quality, experience and outcomes **including risk of direct or indirect discrimination**, and risk to **good relations** between people of different groups?	N/A	
6.	Does the document describe any specific **opportunities to promote equality and human rights**, good relations between people of different groups, to enhance participation, etc.?	N/A	
7.	Does the document describe how the proposal, policy etc. will **address** the **identified inequalities**, and	N/A	
8.	Does the document make recommendations to **mitigate risks** and **enhance the opportunities to promote** equality and equity?	N/A	
9.	Does the document describe how **monitoring and reporting** will take place to assure equality and equity in the future including to stakeholders. [audit and monitoring table may be used]		

* Race/ ethnicity, gender (including gender reassignment) age, religion or belief, disability, sexual orientation, marriage or civil partnership, pregnancy and maternity. This will include groups such as refugees and asylum seekers, new migrants, Gypsy and Traveller communities; and people with long term conditions, hearing or visual impairments, mental health problems or learning disability

14. Data Protection Impact Assessment

No data protection impact assessment is required for this document.

15. Complaints

All requesters are advised of their right to complain to the Information Commissioner's Office, contacted at:

Information Commissioners Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK5AF
Tel: 0303 123 1113
Fax: 01625 524510
Email: casework@iso.gsi.gov.uk

Appendix A - Requests for access to information

Under the Access to Health Records Act 1990, Data Protection Act 2018 and General Data Protection Regulation – as referenced in the DPA 2018

Consent form for the review and release of records containing personal data

What you need to complete:

- Section 1 – Your Details (with as much detail as relevant to help us locate the information)
- Section 2 – Your Information (help us locate the information you're looking for by providing us with a description)
- Section 3 – Your Identity (we ask you to confirm your identity by providing copies of identification documents to help keep your information safe)
- Section 4 – Your Authorisation (your signature and consent to allow us to process your request)

For those requesting details about a deceased individual please complete Section A

For all requests return details are provided in Section 5

Section 1 - Your Details

Full Name		**Former Name(s)**	
Current Address		**Former Address (with date of change)**	
Date of Birth		**NHS Number (if known and relevant)**	
Contact phone number (inc. area code)		**Email address (optional)**	

Section 2 – Your Information

Important Note: Under the Data Protection Act 2018 you do not have to give a reason for applying for access to your personal information. However, under the terms of the Act, as modified by the Freedom of Information Act 2000, c.36, Schedule 6 para. 1, we require you to describe the information you require in order for us to locate that information.

In addition, to help save time and resources, **if you wish**, it would be helpful if you could provide the following information, along with any details you feel are relevant (such as previous names and addresses). The more precise you can be about what information you require, the more efficiently we can provide you with a response.

Please provide an indication of what information you are looking for by **ticking** the relevant boxes

Please indicate what is being applied for:

For members of the public	
❑	I am applying for copies of my health records
❑	I am applying for copies of personal data held in your records
❑	I have instructed my authorised representative to apply on my behalf
❑	I am applying for access to a child's record and have parental responsibility
❑	I am applying for health information of the deceased
For staff	
❑	I am applying for access to personal data held about me by your organisation
Other circumstances (please detail)	
❑	

Please indicate the Borough or County to which your request relates

(Please print all details and use Black Ink)

Date and type of records

When seeking copies of your GP Health Record please contact your GP in the first instance

Section 3 – Your Identity

Where we are unsure of your identity, we will need to ask that the following proof of Identity is required:

(For Adults)

❑	**Good legible photocopies of one type of identification from this list:** ***Passport, driving licence, government issue photo identification, NHS card, tenancy agreement, credit or bank card, birth certificate*.**
❑	One additional proof of address from the following list: ***Rent card or book, benefit book, council tax bill, utility bill, bank or account card statement, letter from a government department or local authority.*** ***All must be dated within the last 3 months.***

Section 3.1 – Requesting a Child's Information

If the patient is a child we require

❑	**Birth certificate**
❑	Proof of parental responsibility (where not evidenced by the birth certificate)

Child's details

Full Name		**Former Name(s)**	
Current Address		**Former Address (with date of change)**	
Date of Birth		**NHS Number (if known and relevant)**	

Section 3.2 – Applying for access for an authorised representative

Representative's details

Name		**Contact Number**	
Representative's Address		**Contact Email**	
		Notes	

Representative's signature	
Date	

For commercial companies: Please provide confirmation of your address by providing a covering note on letter-headed paper with the relevant signature.

For individuals: We may need confirmation of your address and signature, we will advise accordingly on a case-by-case basis.

Section 4 – Your Authorisation

Please read the notes on the following page and confirm: I have read this form and authorise a subject access request to be carried out. I understand that a fee may be required prior to release of any information if there is an excessive administrative exercise. I declare that the information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the personal data detailed above under the Data Protection Act 2018.

Your signature	
Date	

Section 5 – Return Details

Please send this completed form to:

Information Governance Team, NEL, Kent House, 4th Floor, Station Road, Ashford, TN23 1PP

Or by email to: nelcsu.information-governance@nhs.net

Section A – Requesting Health Records of the deceased

Please note the duty of confidentiality to patients extends beyond death and the records you request will be reviewed to establish how far this duty extends. A request to view the records of the deceased is made under the Access to Health Records Act 1990 and proof of the basis of the request may be required.

For members of the public	
❑	I am applying as the patient's personal representative (as executor or administrator of the deceased's estate)
❑	I am have a claim arising from the patient's death (please note this are treated on a case-by-case basis and further details may need to be sought).

Details of the deceased

Full Name		**Former Name(s)**	
Last Address		**Former Address (with date of change)**	
Date of Birth		**NHS Number (if known and relevant)**	

Details of the deceased's GP

Name of Practice	**Name of GP**
Practice Address	

Any other details you may feel are relevant and will help us locate the information

Notes:

You are entitled to receive a copy of the personal data held by us about you. For health records you should also be aware that in certain circumstances your right to see some details in your health records may be limited in your own interest or for other reasons.

You will be entitled to receive a copy of or view your health records within one month of the date that we receive your request and confirm your identity. We aim to acknowledge your request within 1 working day.

Any information you have supplied in making this request will be treated in confidence. It will be used for the purpose of carrying out the search for your information in accordance with Article 15 of General Data Protection Regulation as referenced in the Data Protection Act 2018.

If your request indicates the release of information to a Third Party (e.g. a solicitor, insurance company or relative) please complete the relevant section.

If you are applying for access to your own records, you will need to:

- Complete this form
- Provide the identification specified

Retention of Personal Information

We will keep your personal details on a database for 12 months to help monitor and improve performance. This information will be kept confidential and is subject to the Data Protection Principles. We will only hold this information to enable us to deal with your request and any follow-up issues or complaints. We will not use the information for any other purposes without your permission.

- You do not need to give a reason to access your personal details.
- Please provide as much information as possible, you are required to identify the information you require in order to enable us to locate that information.
- Please ensure that all information provided is accurate and up to date.
- We aim to respond within a maximum of one month to your request

- If access has recently been given, access may not be given until a reasonable time interval has elapsed. What is reasonable depends on the nature of the information, the purposes for which is processed and when it was altered or added to.
- There is no minimum age for applications. Children can apply for their own records provided they are capable of understanding the nature of the request.
- A parent or person with parental responsibility can only apply on the child's behalf if (a) the child has given consent, or (b) the child does not have sufficient understanding to make the request. Please note that a parent does not have a legal right of access to their child's health records.

Appendix B – Standard letter text for acknowledging requests and/or requesting more information

NB. Can be replied to on email if the requester has made the request in that manner

[Insert Date]

Reference: [Insert Reference]

Dear [Name of Requestor],

Subject Access Request received [DATE]

Thank you for your letter/email* received on [DATE] addressed to [NAME], [TEAM], [NAME OF CLIENT] requesting records [IDENTIFY RECORDS REQUESTED HERE]. NHS NEL supports [NAME OF CLIENT] with responding to subject access requests and this letter confirms receipt of your request.

*Please accept our apologies for the delay in acknowledging your request and any inconvenience this may have caused. This was due to… [as appropriate]

*We can confirm that [NAME OF CLIENT] holds the information you have requested. Data Protection legislation requires that personal and sensitive data is released only to those who have a legitimate basis for access to it. We therefore ask for verification of identity to help keep this information safe. Please send us a colour copy of either your passport, driving licence or other official document containing your photograph, as well as an official letter no more than three months old showing your address. If you provide a driving licence, the address details on the licence must match those on the official letter. If you have difficulty in providing these documents, please contact us to discuss suitable alternatives.

*We can confirm that [NAME OF CLIENT] holds the information you have requested. As you have already provided the necessary evidence of identity and/or authority to act, [NAME OF CLIENT] will provide a copy in the format requested.

*If you are requesting a copy of records on behalf of another person, please provide a copy of appropriate documents authorising you to do so. These may include a Power of Attorney or other Court documents naming you and authorising you to act on that person's behalf.

**FOR SOLICITORS ONLY* – Please confirm that the necessary ID checks have been properly carried out, and that you have the data subject's consent to provide the information to your client.

*We can confirm that [NAME OF CLIENT] does not hold the information requested. If you feel this is not correct, please provide details, such as the specific nature of the information required and any relevant dates or time periods.

In the meantime, please contact us if you need further information or clarification about your request.

Yours sincerely,

Name
Job role
*Delete as applicable

Appendix C – Standard letter text enclosing information

NB Can be sent by email if recipient is in agreement. Please use secure email if this is NOT to the data subject

[Insert Date]

Reference: [Insert Reference]

Dear [Name of Requestor],

Subject Access Request received [DATE]

Data Protection legislation (GDPR, Article 15) requires Controllers to provide data subjects with access to personal information access on request. There are some exceptions related to areas such as crime detection and prevention and national security. Further to your subject access request please find enclosed a copy of the records you have requested.

Controllers must also provide additional prescribed information about how your data is processed. The enclosed Privacy Notice therefore explains what kind of information we hold about you and who it is shared with.

We trust this now closes your request. If you have any further questions then please contact us in the first instance. However, if you are not satisfied with the way your subject access request has been handled you can also contact the Information Commissioner's Office at:

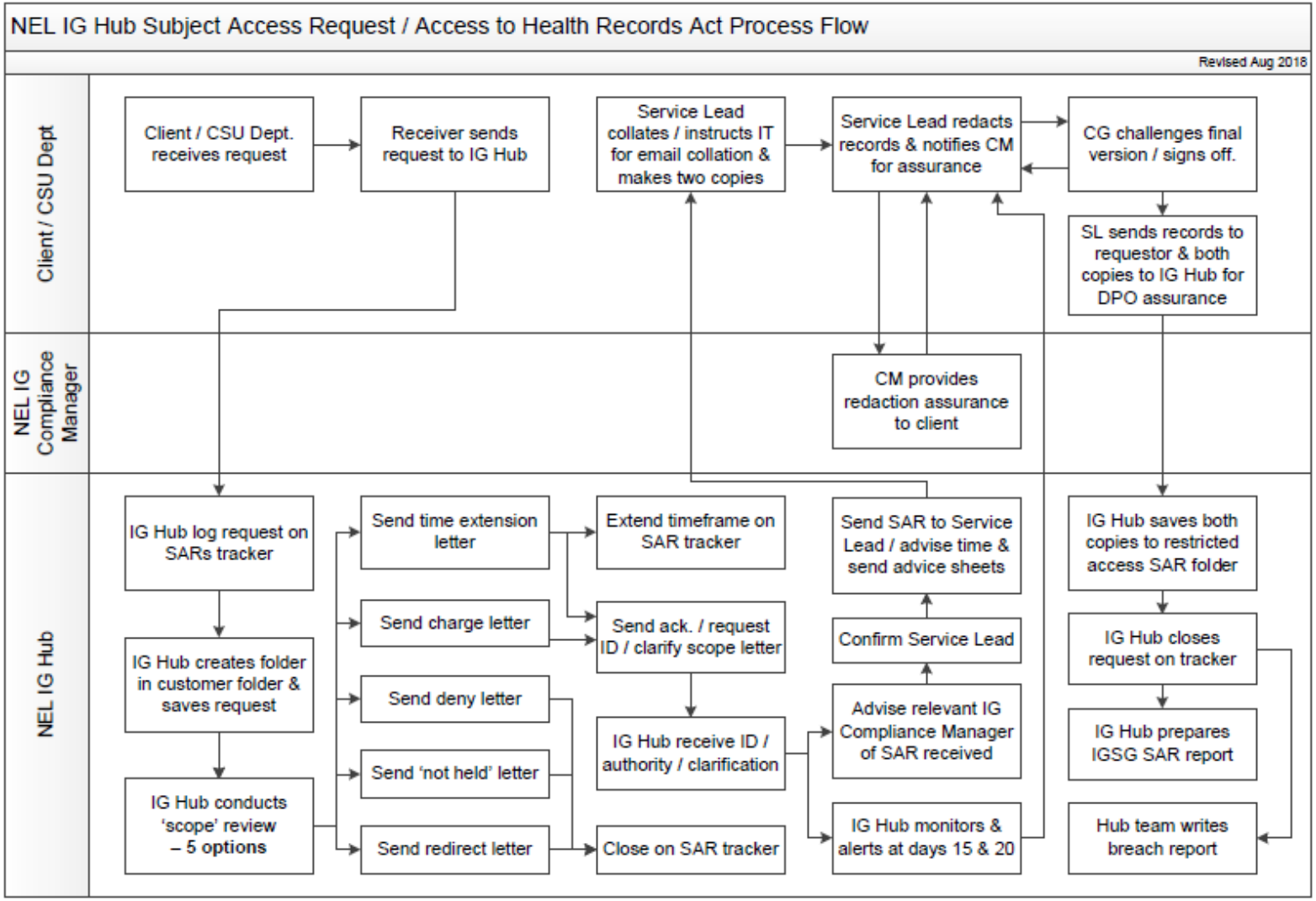
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
Phone: 0303 123 1113 or 01625 545745

Yours sincerely,

Name
Job role

Enc: Privacy Notice

APPENDIX D – PROCESS OVERVIEW


NEL IG Hub Subject Access Request / Access to Health Records Act Process Flow
Revised Aug 2018
Client / CSU Dept
NEL IG Compliance Manager
NEL IG Hub
Client / CSU Dept. receives request
Receiver sends request to IG Hub
Service Lead collates / instructs IT for email collation & makes two copies
Service Lead redacts records & notifies CM for assurance
CG challenges final version / signs off.
SL sends records to requestor & both copies to IG Hub for DPO assurance
CM provides redaction assurance to client
IG Hub log request on SARs tracker
IG Hub creates folder in customer folder & saves request
IG Hub conducts 'scope' review – 5 options
Send time extension letter
Send charge letter
Send deny letter
Send 'not held' letter
Send redirect letter
Extend timeframe on SAR tracker
Send ack. / request ID / clarify scope letter
IG Hub receive ID / authority / clarification
Close on SAR tracker
Send SAR to Service Lead / advise time & send advice sheets
Confirm Service Lead
Advise relevant IG Compliance Manager of SAR received
IG Hub monitors & alerts at days 15 & 20
IG Hub saves both copies to restricted access SAR folder
IG Hub closes request on tracker
IG Hub prepares IGSG SAR report
Hub team writes breach report