Subject Access Procedure and Guidance

Policy Number: **IG11**

Version:	2.3
Approved by:	Information Governance Working Group
Date approved:	May 2018
Ratified by:	Audit and Risk Committee
Date ratified:	July 2018
Name of originator/author:	Louise Chatwyn –Information Manager
Name of responsible individual:	Neil Boughton – Deputy Director of Corporate Affairs
Review date:	May 2020
Target audience:	All Staff of Nene CCG and Corby CCG

Version Control Sheet

Version	Date	Who	Change
Un-numbered	Jan 14	Arden GEM CSU	1st version
2.0	Aug 16	Monica Higgins	Transferred to new template – summary of changes below.
2.1	Sept 16	Louise Chatwyn	Incorporation of consultation comments
2.2	July 17	L Chatwyn	Minor revisions to reflect current legislation and practice and changes under the General Data Protection Regulations (GDPR)
2.3	May 18	L Chatwyn	Revisions to reflect changes in legislation under the General Data Protection Regulations (GDPR) and Data Protection Act Incorporate Corby CCG

Contents

1. Introduction

Robust Information Governance requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources.

Corby and Nene CCGs are public bodies, with information processing as a fundamental part of their purpose. It is important, therefore, that the organisation has a clear and relevant Subject Access Procedure, and that practices are implemented throughout the CCG to ensure compliance with all appropriate legislation, and standards.

The European Union General Data Protection Regulation (GDPR) which was adopted by the European Union in 2016, came into force in all EU Member States from 25 May 2018. GDPR is supplemented by the UK Data Protection Act 2018.

2. Purpose

This document is a statement of the approach and intentions for the CCGs to fulfil their statutory and organisational responsibilities. It will enable management and staff to make correct decisions, work effectively and comply with relevant legislation and the organisations aims and objectives.

Article 15 of the General Data Protection Regulation (GDPR) outlines the Right of access by the Data Subject.

Section 45 of the UK Data Protection Act 2018 defines the Right of access by the data subject.

This is outlined in Section 5 of this document.

This document outlines how the CCGs will handle the rights of Data Subjects, the types of data covered and the process by which information can be released.

3. Scope

This document applies to all staff, whether permanent, temporary or contracted. They are responsible for ensuring that they are aware of all relevant requirements and that they comply with them on a day to day basis.

Furthermore, the principles of this document apply to all third parties and others authorised to undertake work on behalf of the CCGs.

This document applies to all requests for access to personal data held by either CCG.

4. Key Roles and Responsibilities

Role	Responsibility
Accountable Officer	The Accountable Officer and the Board have ultimate accountability for actions and inactions in relation to this document
Senior Information Risk Officer	The CCG's SIRO is responsible for having overall accountability for Information Governance; this includes the Data Protection and Confidentiality function. The role includes briefing the Board and providing assurance through the Audit and Risk Committee that the IG approach is effective in terms of resource, commitment and execution. The SIRO for Corby CCG and Nene CCG is the Chief Finance Officer
Caldicott Guardian	The Caldicott Guardian has responsibility for ensuring that there are adequate standards for protecting patient information and that all data transfers are undertaken in accordance with Safe Haven guidelines and the Caldicott principles. The Caldicott Guardian for Corby CCG is a Clinical Executive The Caldicott Guardian for Nene CCG is the GP Chair
Data Protection Officer	The DPO has responsibility for Data Protection compliance The DPO role for the CCGs is fulfilled by NEL CSU Email: nelcsu.dpo@nhs.net Phone: 03000 428438
Deputy Director of Corporate Affairs	The Deputy Director of Corporate Affairs has overall day to day responsibility for the Information Governance in the CCG. The role includes briefing the Board, including the SIRO and Caldicott Guardians of information risks and information incidents

Information Manager	The Information Manager has day to day responsibility for implementing and monitoring procedures to ensure compliance with relevant information legislation The Information Manager is responsible for completion of the annual Data Security and Protection Toolkit, actions arising to ensure compliance and subsequent workplans for continuing improvement
Managers	Managers and supervisors are responsible for • ensuring that staff who report to them have suitable access to this document and it's supporting policies and procedures and that they are implemented in their area of authority • ensuring the initial training compliance of all staff reporting to them
All staff	Have a responsibility to: • Be aware of the Information Governance requirements • Support the CCG to achieve Toolkit Compliance • Complete annual Data Security and Protection training • Report information Incidents appropriately

5. Subject Access Requests (SAR) – the rights of access by the data subject

Article 15 of the General Data Protection Regulation (GDPR) outlines the Right of access by the Data Subject.

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
    (a) the purposes of the processing;
    (b) the categories of personal data concerned;
    (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
    (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
    (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
    (f) the right to lodge a complaint with a supervisory authority;
    (g) where the personal data are not collected from the data subject, any available information as to their source;
    (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful

information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Section 45 of the UK Data Protection Act 2018 sets out the right of access to data subjects and the information that should be disclosed on request

(1) A data subject is entitled to obtain from the controller—
- (a) The Data Protection Act provides that a data subject is entitled to obtain from the controller Confirmation as to whether or not personal data concerning him or her is being processed, and
- (b) Where that is the case, access to the personal data and the information set out in subsection (2)

(2) That information is –
- (a) the purposes of and legal basis for the processing
- (b) the categories of personal data concerned
- (c) the recipients or categories of recipients to whom the personal data has been disclosed (including recipients or categories of recipients in third countries or international organisations)
- (d) the period for which it is envisaged that the personal data will be stored or, where that is not possible, the criteria used to determine that period
- (e) the existence of a data subject's rights to request from the controller
  - I. rectification of personal data (section 46) and
  - II. erasure of personal data or the restriction of processing (section 47)
- (f) the existence of the data subject's right to lodge a complaint with the Commissioner and the contact details of the Commissioner
- (g) communication of the personal data undergoing processing and of any available information as to its origin

(3) Where a data subject makes a request under subsection (1), the information to which the data subject is entitled must be provided in writing —
- (a) without undue delay, and
- (b) in any event, before the end of the applicable time period[3] (as to which see section 54).

5.1 Form of provision of information

Section 52 of the UK Data Protection Act 2018

(1) The controller must take reasonable steps to ensure that any information that is required by this Chapter to be provided to the data subject is provided in a concise, intelligible and easily accessible form, using clear and plain language.

[3] "The applicable time period" means the period of one month, or such longer period as may be specified in regulations, beginning with the relevant day.

(2) Subject to subsection (3), the information may be provided in any form, including electronic form.
(3) Where information is provided in response to a request by the data subject under section 45, 46, 47 or 50, the controller must provide the information in the same form as the request where it is practicable to do so.

6. Refusing a request

Section 45 of the UK Data Protection Act 2018 – Subsections

(4) The controller may restrict, wholly or partly, the rights conferred by subsection (1) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to—

(a) avoid obstructing an official or legal inquiry, investigation or procedure;
(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
(c) protect public security;
(d) protect national security;
(e) protect the rights and freedoms of others.

(5) Where the rights of a data subject under subsection (1) are restricted, wholly or partly, the controller must inform the data subject in writing without undue delay—
(a) that the rights of the data subject have been restricted,
(b) of the reasons for the restriction,
(c) of the data subject's right to make a request to the Commissioner under section 51,
(d) of the data subject's right to lodge a complaint with the Commissioner, and
(e) of the data subject's right to apply to a court under section 165.

(6) Subsection (5)(a) and (b) do not apply to the extent that the provision of the information would undermine the purpose of the restriction.

Article 15 of the General Data Protection Regulation (GDPR) states that the rights of the data subject shall not adversely affect the rights and freedoms of others.

7. Where to send requests

All requests must be made in writing by the applicant. Where an application is made on behalf of an individual, an authorisation letter must accompany the written application.

On receipt by the CCG all requests must initially be logged and assessed by the Information Team.

The CCGs recognise that as Clinical Commissioning Groups they do not have legal rights to personal confidential data for commissioning purposes and will use de-identified and aggregated data for that purpose.

As the CCGs use a Commissioning Support Unit (CSU) to support a number of their activities, requests received may then need to be passed onto a third party who holds the information and will process the request.

Request relating to	**Processed by**	**Reviewer**#
Staff members HR records	CSU HR team	Information team
Employees payroll information	CSU HR team	Information team
Complaints	CSU Complaint department	Complaints Manager
Adult Continuing Health Care (CHC)	CSU Adult CHC team. Requests are usually sent directly to the CSU by the requester.	Clinician
Children & Young People Complex and Continuing Care	Nene CCG Children and Young People's team	Clinician
Individual Funding Requests (IFR)	CSU IFR team	Clinician
Other	Nene and Corby Corporate Services	Information Team

Any request sent to a third party for processing should state the day it is received and the day by which it should be completed for release.

8. Types of Records

8.1 Health Records

A health record is defined as:

- Consisting of information relating to the physical or mental health or condition of an individual
- **and** has been made by or on behalf of a health professional in connection with the care of that individual

8.2 Shared Records

There are situations where a subject access request involves a health record that is shared between healthcare organisations.

The modernisation and integration of health and social care will place a greater emphasis on shared records. In developing integrated health and social care service, the CCGs will set out its arrangements for managing the requirements of

the Data Protection Regulations and Subject Access requests with its partners as part of any service reconfiguration or development.

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

- Obligations under the Regulations are, in general placed on the holder of the record. If records are shared between two health or NHS bodies, they will be joint data controllers. Responsibility for ownership of the record rests with the Secretary of State for Health although essentially, where both organisations are joint data controllers for the shared record, both are controlling how they are used
- In order to deal with Subject Access requests effectively, the organisation receiving the Subject Access request will take responsibility for processing the request and for obtaining consent or refusal for the release of parts of the record relating to the other organisation
- The CCG is obliged to deal with the access request and the authorisation to release the parts of the record in order to ensure the request is processed within the applicable time period of one month as required by the Data protection Regulations
- The CCG takes responsibility for the access request and joint liability for their release where each organisation has authorised its release
- If the CCG does not agree with the decision made by the other organisation to withhold data from release and subsequently releases that element of the record, it will accept full liability
- The CCG must document the reasons for withholding certain information lawfully in the request log. The applicant may challenge the decision not to release information
- If there is a refusal to disclose the record from the partner organisation, the organisation dealing with the access request should, in their response to the applicant explain the reason for the refusal and refer them to the other partner organisation directly if they wish to contest the refusal.

8.3 Other Records

In addition to health records, all other records held by the CCGs containing individual's information are liable to subject access requests by those individuals or their representatives. This includes personnel, finance, complaints and administration records. Any 'third party' content of the record must be referred to the originating organisation for consent to release.

8.4 Deceased Patient Records

The right to access under the Data Protection Regulations extends only to living individuals (classified as natural persons under the Regulations). Requests for

deceased patients' records are made under the Access to Health Records Act 1990[4]. Requests can only be made by:

- The patient's personal representative (usually the executor of the will or administrator of the estate) or
- Any person who may have a claim arising out of the patient's death- release of any information will only be the minimum necessary to process their claim. Only relevant information relating to any claim made should be released

In order to show that the Applicant has been appointed as the personal representative the CCG will ask for a copy of the Grant of Probate or Letters of Administration. The CCG understands that these documents are not always available so will accept requests from the next of kin providing they have proof of identity and taking into account the patient's wishes before they died. The CCG will also consider the confidentiality principles when releasing this information. For more information please read *'Guidance for Access to Health Records Requests February 2010'*, which can be accessed on http://systems.hscic.gov.uk/infogov/links/dhaccessrecs.pdf.

The personal representative is the only person who has an unqualified right of access to a deceased patient's record and need give no reason for applying for access to a record. Individuals other than the personal representative have a legal right of access under the Act only where they can establish a claim arising from a patient's death.

There is less clarity regarding which individuals may have a claim arising out of the patient's death. Whilst this is accepted to encompass those with a financial claim, determining who these individuals are and whether there are any other types of claim is not straightforward. The decision as to whether a claim actually exists lies with the record holder. In cases where it is not clear whether a claim arises the record holder should seek legal advice.

Record holders must satisfy themselves as to the identity of applicants who should provide as much information to identify themselves as possible. Where an application is being made on the basis of a claim arising from the deceased's death, applicants must provide evidence to support their claim. Personal representatives will also need to provide evidence of identity.

A health professional must inspect records taking into account the following:

- If it is known whether the deceased patient did not wish for their records to be disclosed or the records contain information that the deceased patient expected to remain confidential

[4] http://www.legislation.gov.uk/ukpga/1990/23/contents

- If the release of the information is likely to cause serious harm to the physical or mental health of any individual
- The same rules apply to third party information as with other health records. The CCG should afford the same level of confidentiality to deceased patient's records as for living ones.

9. Requests from public bodies and law enforcement agencies

In certain circumstances the CCGs are required by law to release information in support of the legal obligations bestowed on them. The General Data Protection Regulation 2016 allows CCGs to release information where it is believed by not releasing would be in contravention of its legal duties. This is contained in;

Article 23(1)(d) - The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

The legal duties are as follows;

Police and Criminal Evidence Act 1984 – Sections 19 & 20.
Terrorism Act – Sections 19 & 39.
Fraud Act 2006 – Section 1
Computer Misuse Act – Section 1 now the Police and Justice Act 2006 section 35
Serious Crime Act 2007 – Section 68 & 72

The CCG as a data controller must still exercise caution when releasing personal data to such parties. A formal documented request signed by an appropriately senior officer of the relevant authority is required to initiate the request.

The request must explicitly state which of the above are being relied upon and that not receiving the information would prejudice the investigation.

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

This type of disclosure may only be authorised by the SIRO or Caldicott Guardian.

It should be noted that the Data Protection Act 2018 exempts the controller from informing the data subject when some criminal, tax and immigration activities are followed up by the police and other UK law upholding bodies.

All such requests **must be passed to the Information team immediately**.

10. Consent

In most cases the consent to access personal information will be provided by the individual who is requesting the information.

A third party, e.g. solicitor may make a valid SAR on behalf of an individual. However, where a request is made by a third party on behalf of another living individual, appropriate and adequate proof of that individuals consent or evidence of a legal right to act on behalf of that individual e.g. power of attorney must be provided by the third party.

If you think an individual may not understand what information would be disclosed to a third party who has made a SAR on their behalf, you may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

10.1 Children

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

Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. If the clinician responsible for the child's treatment plan is confident that the child can be considered competent under Gillick/Fraser guidelines, has the capacity to understand their rights and any implications of the disclosure of information, then child's permission should be sought to action the request.

The GDPR states that, if consent is your basis for processing the child's personal data, a child under the age of 16 can't give that consent themselves and instead consent is required from a person holding 'parental responsibility' – but note that it does permit member states to provide for a lower age in law, as long as it is not below 13.

11. Exemptions to the Release of information

Data Protection Act Regulations makes provision for withholding information in certain circumstances which must be considered when a request is received.

GDPR Article 15, paragraph 4 states that the rights of the data subject shall not adversely affect the rights and freedoms of others.

For advice on exemptions which may apply you should contact the CCG Information Team. Some examples are outlined below:

11.1 Data identifying a Third Party

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

11.2 Serious harm or adverse effect on health

On inspection of the records the health professional can advise that certain personal information is not released on the grounds that its release would be likely to cause serious harm to the physical or mental health of the patient or to others. There is no definite requirement to inform the patient or their representative that this information has not been released.

11.3 Other Agencies Records

Letters or reports from another agency or person may be contained in a patient's records. Where this is the case the health professional inspecting the records should consider the need to approach those agencies or persons to secure agreement for release of those records.

If information has been obtained from another NHS organisation and used for direct care purposes there is no obligation to contact the other organisation for permission to release (but there may be circumstances where this may need to be considered).

12. Failure to Comply

Any failure to comply and/or breaches of this Policy and associated procedures and guidelines will be investigated thoroughly in accordance with the organisation's disciplinary policies.

Any incident involving a potential breach of the Data Protection Regulations or the Access to Health Records Act 1990 should be reported as an incident using the Toolkit reporting system.

Your line manager and the Caldicott Guardian should also be informed of this and a decision will be taken whether it is necessary to report this as a Serious Incident under the Serious Incident Reporting and Management Policy and/or to the Information Commissioner.

Failure to comply with a request for subject access, without valid justification is treated as a serious matter and is investigated by the Information Commissioner. Such complaints are dealt with as a matter of priority and may often lead to a full scale investigation into an organisation's procedures and practices.

13. Monitoring and Review

Performance against key performance indicators will be reviewed on an annual basis through the DSP Toolkit submission and used to inform the development of future documents.

Toolkit Data Security Standard 1.3.5 and 1.3.6

There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data.

Record of number of received SARs will be reported to the Information Governance Working Group on a quarterly basis.

Unless there is major legislation or policy changes, this document will be reviewed every two years.

14. Training

Appropriate training will be provided to all Staff commensurate with their role profile as necessary.

Training is available through ESR which can be found here:
http://www.esrsupport.co.uk/access.php

15. Distribution and Implementation

A full set of policy and procedural documents to support Information Governance will be made available via the Nene CCG staff intranet.

Staff will be made aware of procedural updates as they occur via team briefs, management communications, shared drive availability and notification via the CCG staff intranet where this is in place.

16. Associated Legislation and Documents

To include but not limited to:

- IG01a – Framework CSU Information Governance Framework
- IG01b – Policy CSU Information Governance Policy
- IG02a – CCG Physical Assets
- IG02b – Data Assets (application provider guide)
- IG03 – CCG Information Disclosure and Sharing Policy and Procedure
- IG04 – CCG Email and Internet
- IG05 – CCG Data Security and Protection Incident Procedure
- IG06 – CSU Confidentiality & Data Protection Policy
- IG07 – CCG/CSU Data Protection Impact Assessment Procedure
- IG08a – Framework CSU Information Security Framework

- IG08b – CCG Information Security Policy
- IG09 – CCG Safe Haven Procedure
- IG10a – Framework CSU Information Quality Framework
- IG10b – CCG Records Management Policy
  IG12 – CSU Freedom of Information Policy and Procedure

The following references and areas of legislation should be adhered to.

- Confidentiality NHS Code of Practice
- Common law duty of confidentiality
- General Data Protection Regulations GDPR
- UK Data Protection Act
- Caldicott Guardian principles
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Access to Health Records 1990
- Records Management NHS Code of Practice
- Department of Health Records Management NHS Code of Practice
- Human Rights Act 1998
- Information Commissioner's Office (ICO) Subject Access Code of Practice

There is also a requirement that organisations respect people's private lives unless there is a lawful exemption to the Human Rights requirements and that information obtained in confidence should not normally be used in an identifiable form without the permission of the service user concerned.

17. References

Data Security and Protection Toolkit
https://www.dsptoolkit.nhs.uk/

EU General Data Protection Regulation (GDPR)
https://www.eugdpr.org/

Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

NHS Code of Confidentiality
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf

The Caldicott Review: Information Governance in the Health and Social Care System
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

Access to Health Records Act 1990
http://www.legislation.gov.uk/ukpga/1990/23/contents

Human Rights Act 1998
http://www.legislation.gov.uk/ukpga/1998/42/contents

Records Management Code of Practice for Health and Social Care 2016
available from http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf

Information Commissioner's Office (ICO) Subject Access Code of Practice
https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf

18. Appendices

Appendix 1 Subject Access Process

1. Receiving an access request

Applications for access to personal data should be made in writing, signed and dated, and forwarded on the day of receipt, to:

Information Team
NHS Nene CCG
Francis Crick House
Summerhouse Road
Moulton Park
Northampton
NN3 6BF
Nccg.informationgovernance@nhs.net

The application must clearly identify the Data Subject, and the records required, including the following details:

- Full name – including previous names
- Address – including previous address(es)
- NHS number (if available)
- Date of birth
- Dates of health/personnel records required

2. Response times for disclosure

Responses to request for access must be made within one month of the date of receipt of the request
Failure to do so is a breach of the Regulation and could lead to a complaint to the Information Commissioner. In exceptional circumstances, if it is not possible to comply with this period, the applicant should be informed.

3. Provision of Information

The CCG will take into account the provisions of the Equality Act 2010 and offer

- Information in large print or Braille format
- Data Subjects to view their data

All copies of information released will be in an intelligible form and the use of jargon, abbreviations or codes contained within the information will be explained.

If the information is terminologically difficult or of a technical nature, the CCG will offer a meeting with the Data Subject to explain the meanings.

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

Where the CCG does not hold the personal information requested, it will inform the applicant as quickly as possible.