NHS
Birmingham and Solihull
Clinical Commissioning Group

Data Protection & Confidentiality Policy

Version:	Version 2.0
Ratified by:	Corporate Management Team
Date ratified:	13th March 2020
Name of originator/author:	Nigel Parr, Senior Information Governance Manager
Name of responsible committee/individual:	Information Governance Steering Group
Name of executive lead:	Dr Richard Mendelsohn, Caldicott Guardian
Date issued:	20th March 2020
Review date:	March 2022
Target audience:	All Staff

Review and amendment log

Version no	Type of change	Date	Description of change
1.0		26/03/19	Creation of Policy
1.1	Full review of Policy	15/01/20	Creation of policy statements in respect of key areas of Data Protection – updated to reflect GDPR and specific procedures adopted by the CCG – endorsed by IG Steering Group
2.0	Approval	13/03/20	Approved by Corporate Management Team

Contents

POLICY OVERVIEW

Purpose

The purpose of the Data Protection & Confidentiality (DP) Policy is to set out NHS Birmingham and Solihull Clinical Commissioning Group's (CCG) approach to compliance with Data Protection legislation. The DP Policy is primarily designed to ensure that the CCG:

- Has compliance statements in key areas of Data Protection legislation;
- Does not breach the common law duty of confidence;
- Has adequate policies and procedures to manage Data Protection risk;
- Has standards for employees to follow, if their role requires access to personal data,
- Meets the requirements of the NHS 'Caldicott Principles'

Who this policy applies to

This policy applies to all CCG employees, office holders, CSU embedded staff and contractors ('employees') who have access to any personal data for which the CCG is the 'data controller'. Employees who access personal data must therefore ensure that they are aware of and follow the requirements of this policy. In addition, some employees have key responsibilities:

Senior Information Risk Owner (SIRO) - The SIRO is the Chief Information Officer and chairs the CCG's Information Governance Steering Group. The SIRO is accountable for information governance risk within the CCG.

Caldicott Guardian (CG) – The CG is the Chief Medical Officer, who acts as the point of escalation in respect of matters affecting patient confidentiality. The CG also acts as the "conscience" of the CCG in respect of the sharing and use of patient information.

Data Protection Officer (DPO) – The DPO is the CCG Solicitor, who monitors internal compliance and reviews Data Protection Impact Assessments.

Senior Information Governance Manager (SIGM) - The SIGM is responsible for making sure that the CCG has adequate policies and procedures in place to comply with Data Protection legislation and satisfy the Data Protection requirements of the Data Security and Protection (DSP) Toolkit. The SIGM is also responsible for managing Data Protection breaches and reporting associated risks to the SIRO and CG, as well as responding to all correspondence from the Information Commissioner's Office (ICO).

Legal and regulatory considerations

This policy is designed to reflect the following legislation and mandatory NHS standards

- General Data Protection Regulation;
- The Data Protection Act 2018;
- Privacy and Electronic Communications Regulations 2003;
- Human Rights Act 1998;
- Caldicott Principles;
- Section 251 of the NHS Act 2006, which allow the Secretary of State to make regulations to set aside the common law duty of confidentiality, where it is not possible

to use anonymised information and where seeking consent is not practicable ('section 251 approval').

The GDPR lists the following categories of personal data:

- Personal data – information about an individual who can be identified by reference to an identifier such as name, identification number and online identifier.
- 'Special Category' Personal Data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, biometric data, data concerning health or sexual orientation.
- Personal data about criminal convictions.

As a body chiefly responsible for commissioning services, the CCG does not routinely access personal data. However, personal data and special category personal data will primarily be held or accessed by Continuing Healthcare, Medicines Management, Nursing and Quality and Safeguarding.

Personal data can only be processed where the following applies:

- Personal data – The CCG can satisfy a condition listed at Article 6 of the GDPR
- Special category personal data – The CCG can satisfy a condition listed at Article 9 (2) of the GDPR
- Criminal Convictions – The CCG can satisfy a condition listed in parts 1-3 of Schedule 1 of the DPA

These conditions are known as the 'lawful basis for processing'. In addition, the GDPR contains the following obligations:

- Data controllers must report certain types of Data Protection breaches to the independent regulator, the ICO, with 72 hours;
- The GDPR contains large fines for non-compliance, up to a maximum of 20 million euros or 4% of a data controller's annual turnover, whichever is greater;
- Data Protection Impact Assessments must be completed where use of personal data poses a significant risk to individuals' privacy;
- Data controllers must publish detailed information about their uses of personal data, including the lawful basis for processing personal data, the rights individuals have in respect of their personal data and retention of personal data.

Data Protection and Confidentiality Policy

1 – Data Protection Principles

The GDPR contains seven principles, which support the use of personal data. The CCG has to comply with these principles, which require personal data to be:

- Processed lawfully, fairly and in a transparent manner **('lawfulness, fairness and transparency')**;
- Collected for specified, explicit and legitimate purposes **('purpose limitation');**
- Adequate, relevant and not excessive **('data minimisation')**;
- Accurate and, where necessary, kept up to date **('accuracy'**);
- Kept in a form which permits identification of individuals for no longer than is necessary **('storage limitation')**;
- Processed in a manner that ensures that appropriate technical and organisational measures are deployed to protect personal data **('integrity and confidentiality').**

The CCG is also obliged to demonstrate that adequate measures are in place to comply with the above requirements **('accountability').**

The CCG will meet these requirements in the following ways.

Lawfulness, Fairness and Transparency - The CCG will notify individuals of the purposes for which their personal data will be used in the following ways:

- Where personal data is collected directly from individuals, basic information about data use will be provided within the online or other form used to collect the data, with a reference to the CCG's main Privacy Notice included.
- Maintaining an up-to-date Privacy Notice, providing the following as minimum:
    - The personal data the CCG uses and lawful basis for processing;
    - Individuals' rights in respect of their personal data;
    - The CCG's retention of personal data;
    - Transfers of personal data outside the European Economic Area (EEA);
    - Use of third parties (data processors) to process personal data;
    - The right of individuals to seek reviews of the CCG's processing of personal data via the Information Commissioner's Office (ICO).

The SIGM is responsible for maintaining the CCG's Privacy Notice and ensuring that it contains sufficient information to satisfy the requirements of the GDPR and that it is reviewed on an annual basis.

Teams are responsible for ensuring that their use of personal data is referenced within the Privacy Notice and notifying nhsbsolccg.ig@nhs.net if any of their use of personal data are not referenced within it.

The CCG will publish the lawful basis for processing personal data supporting the uses of personal data within our Privacy Notice. Teams are responsible for ensuring that any processing of personal data is supported by a relevant basis for processing and seeking advice from the SIGM where necessary. Where the consent of individuals is relied on to process personal data, the CCG will ensure that:

- The uses of personal data individuals are consenting to are clearly explained;
- That a pro-active action is required to signify consent;
- That the consent is for specific and limited purposes;
- Consent is as easy to withdraw as it is to provide.

Where any processing of personal data relies on consent obtained by a third party, this must be approved by the Senior Information Risk Owner (SIRO).

Principle 2 – Purpose Limitation - The CCG will meet the requirement to limit uses of personal data about patients by:

- Ensuring that personal data is only used to support the statutory services the CCG either provides directly or commissions, or;
- Where the above does not apply, where section 251 approval permits the use of the data without the informed consent of patients, or the CCG obtains the information consent of patients to support the use of their personal data.

Principle 3 – Data Minimisation – In addition, to the controls listed above, the CCG will satisfy data minimisation requirements by:

- Using the minimum personal data necessary to support the business objective and, where possible, use anonymised or pseudonymised data to support these objectives (e.g. to undertake Business Intelligence functions);
- Making individuals aware of how they can opt-out of uses of their personal data;
- Undertaking Data Protection Impact Assessments (DPIAs) for new projects involving significant uses of personal data, to ensure that risks to individuals' privacy are mitigated and that any use of personal data is strictly necessary;
- Ensure that access to personal data is strictly controlled and regularly reviewed.

Principle 4 – Accuracy - The CCG will regularly review personal data to check it remains accurate and up-to-date and that retention remains necessary. The CCG will undertake appropriate data quality audits to check that processes to ensure data quality remain sufficient.

Principle 5– Storage Limitation - Personal data will be retained for no longer than is necessary and accordance with the CCG's retention schedule, which will reflect (insert standard). The CCG will publish the retention periods for specific types of personal data within our Privacy Notice.

The CCG may retain personal data held in a pseudonymised form, where this is necessary to undertake research and a continued use of the data to improve patient services is identified. The retention of any pseudonymised data will be reviewed at least every five years.

Principle 6 – Integrity and Confidentiality - The CCG will protect the integrity and confidentiality of personal data by maintaining a security system which meets the requirement of the Data Security and Protection (DSP) Toolkit and will aim for a submission rated as 'standards exceeded' by March 2022.

The CCG will also maintain a security management system consistent with the requirements of the international information security standard ISO 27001:2013 and will deploy the following security controls:

- Using ‘pseudonymised’ data and encryption techniques, where possible, to enhance the privacy of personal data, particularly in respect of the CCG’s use of personal data to support Business Intelligence functions**;**
- Maintaining procedures to manage breaches of personal data, including criteria for notifying the ICO and individuals that a breach has occurred;
- Maintaining security and governance standards in respect of the use of third party ‘data processors’, process personal data on the CCG’s behalf;
- Maintaining and enforcing an ‘Acceptable Use Policy’, setting out expected standards in respect of employees’ use of confidential and personal data**.**

Employees must be aware of these requirements and ensure that any use of personal data satisfies the requirements outlined above, contacting nhsbsolccg.ig@nhs.net where any uncertainty exists.

2 Individuals’ Rights

The GDPR provides individuals with a number significant number of rights in respect of their personal data, including right to request deletion of their data, access their data, to restrict processing, challenge the accuracy of their data, prevent its use for marketing purposes and automated uses.

Any request by a patient to enforce their rights under the GDPR will be managed by the SIGM and employees must immediately forward requests that they receive directly to nhsbsolccg.ig@nhs.net. The request will be managed by the SIGM within no later than twenty-eight calendar days.

Requests for deletion will typically be declined, where their personal data is held in respect of services the CCG is legally required to provided, or where the information is held for the purposes of research and is retained in pseudonymised form.

Requests to access personal data (Subject Access Requests) will be processed in accordance with the CCG’s Subject Access Procedure.

3 Data Processors

The CCG may use third parties (‘data processors’) to provide services which involve the use of personal data, typically either hosting data on the CCG’s behalf of delivering a service the CCG is legally required to provide. Any new, or renewed, uses of data processors must be supported by the following governance controls:

- The data processor’s use of personal data, and the type of data, must be documented within a formal agreement;
- The data processor must have a current DSP Toolkit Submission of at least ‘standards met’;
- Be able to demonstrate information security standards, either through proof of accreditation to International Information Security Standards, e.g. ISO 27001:2013 (Information Security) or ISO 27018:2014 (Protection of Personal Data in Public Clouds) or through the completion of security questionnaires approved by the Digital Security Operational Manager (DSOM) and SIGM;

- The use of the data processor will be approved by the CCG's SIRO and CG.

The SIGM will produce a register of the CCG's data processors, including the service provided and the governance controls in place. Any employee who intends to use a data processor to support delivery of services, must contact nhsbsolccg.ig@nhs.net.

4 Disclosure of Personal Data and Transfers outside the UK or EEA

Personal data will not be transferred (including hosting) outside of the UK or European Economic Area, without the consent of the data subject, unless the following circumstances apply:

- It supports the CCG's statutory functions and provides significant benefit to the CCG or patients;
- Adequate safeguards, such as contractual clauses, have been included within any agreement with the third party receiving the personal data;
- The SIGM and DSOM have assessed the security standards of the recipient of the data;
- The transfer has been approved by the SIRO and CG.

Where employees are authorised to share personal data (e.g. patient name, NHS number, date of birth, medical records) with third parties, they must not do so via email unless one of the following circumstances apply:

- The email is sent to an nhs.net account;
- The email is sent to another secure email account (e.g. government secure internet – gsi.gov.uk). See 'Use of Email – Good Practice Guidance' for more information;
- The subject of the personal data has consented to the information being sent via non secure email (e.g. to receive information following a request to access personal data);
- The personal data is sent using the NHS mail encrypted email service.

Where the disclosure relates to more than ten individuals, this should only occur via email with the approval of the SIGM, or via an authorised secure file transfer protocol, e.g. NHS Digital approved, or secure file transfer software approved by the SIGM and DSOM.

5 Privacy by Design

All new projects and systems which are implemented, that involve significant use of personal data be supported by a Data Protection Impact Assessment (DPIA). The DPIA will identify the following:

- The purpose of the use of personal data;
- The lawful basis for the use;
- Privacy risks to individuals and mitigation;
- The disclosures and flows of personal data;

DPIAs will be shared with the Information Governance Steering Group for review.

6 Data Protection Breaches

Where it is identified that personal data is disclosed to, or accessed by, any person or organisation not entitled to see it, this must be reported to the SIGM immediately. The breach will be managed in accordance with the CCG's Data Protection Breach Procedure.

7 National Data Opt-Out

The National Data Opt-Out Programme, operational from March 2020, allows patients to opt-out of uses of their data, for purposes other than direct care. The CCG will notify patients of this right via the privacy notice.

The National Data Opt-Out is applied by NHS Digital at source and will therefore be applied prior to receipt of data processed for the CCG's Business Intelligence functions.

8 Employee Training

All CGG employees and Board Members will be required to undertake online Data Security training on an annual basis. The SIGM will identify employees who are access personal data on a regular basis and provide additional classroom based training at least every two years.

9 Further information

For further information or clarification in respect of this policy, please contact nhsbsolccg.ig@nhs.net.