NHS
Bolton Clinical Commissioning Group

Privacy Notice for Patients and Public

Informing you how we Use and Protect Your Data

Contents

Introduction 4
Who are we and what do we do? 4
Definitions of data types processed at the CCG 5
Personal Data 5
Special Categories of Personal Data (previously known as Sensitive Data) 5
Personal Confidential Data 5
Pseudonymised Data or Coded Data 6
Anonymised Data 6
Aggregated Data 6
Primary Care Data 6
Secondary Care Data 6
Secondary Uses Service (SUS) Data 6
Community Care / Social Care Data 7
Data Controller 7
Data Processor 7
Our data processing activities 7
NHS Continuing Healthcare (CHC) applications 7
NHS Continuing Healthcare (CHC) Verifying Patients 8
Individual Funding Requests 8
Safeguarding 9
Incident Management – Serious Incidents 9
Supporting Medicines Optimisation 10
Business Intelligence 11
Secondary use of Data 11
Section 251 of the NHS Act 2006 12
NHS Digital / Data Services for Commissioners Regional Office (DSCRO) 12
Risk Stratification 14
Invoice Validation 16
Purposes where consent is required 17
Patient and public involvement 17
Right of Access Requests (also known as Subject Access Requests) 18
Incidents (non-serious) relating to CCG commissioned services 18
Complaints relating to the CCG 18

Complaints relating to CCG commissioned services 19
Other Partner Organisations 20
Using anonymous or aggregate information 20
How we protect your personal data 21
How long do we keep your personal data (Retention and Destruction? 22
Retention 22
Destruction 22
Who we share your data with? 22
Where is your data processed? 23
What are your rights over your personal data? 23
Right to be Informed 24
Right of Access 24
Right to Rectification 25
Right to Erasure ('forgotten') 25
Right to Data Portability 25
Right not to be subject to a decision based solely on automated processing 25
Right to object to processing 26
Objections to processing for secondary care purposes 26
Complaints / Contacting the Regulator 27
Data Protection Registration 27
Data Security and Protection Toolkit 28
Further Information / Contact Us 28
Links 28

Introduction

This privacy notice explains in detail the type of information (including personal data) that we, Bolton CCG, process about you. The CCG is a Data Controller. A Data Controller determines how the data will be processed and used within the CCG and with others who we share data with. We are legally responsible for ensuring that all personal data that we hold and use is done so in a way that meets the data protection principles under the General Data Protection Regulation (GDPR) and Data Protection Act 2018. We need to ensure that where we process personal data we can do so legally. Article 6 of the GDPR lists 6 lawful bases for processing personal data, at least one must apply. This notice will detail the legal bases for each area where we process personal data and in addition explains how we handle that data and keep it safe.

The CCG has appointed a Caldicott Guardian and Data Protection Officer to safeguard your personal data and support your rights.

A Caldicott Guardian is a senior person within a health and social care organisation, a health professional, who makes sure that personal information about those who use its services is used legally, ethically, appropriately and that confidentiality is maintained. The Caldicott Guardian for the CCG is:

Dr Jane Bradford, Clinical Director - you can contact Jane at Bolccg.communications@nhs.net (please note this email account is accessed by a number of personnel therefore consider the information provided when contacting and please state that the email is for the Caldicott Guardian of Bolton CCG).

A Data Protection Officer ('DPO') is a senior person who is an expert in data protection and can therefore inform and advise the CCG and its staff about their obligations to comply with the GDPR and other data protection laws. Where issues arise they will act as your single point of access. The DPO for the CCG is:

Michael Robinson, Associate Director of Governance and Safety
Email: michael.robinson1@nhs.net

We will continually review and update this privacy notice to reflect changes in our services and to comply with changes in the law. When such changes occur, we will revise the last updated date as documented in the version status in the footer of this document.

Who are we and what do we do?

Bolton CCG is an NHS commissioning organisation. We are responsible for planning, buying and monitoring (also known as commissioning) health services from healthcare providers such as hospitals and GP Practices, for our local population to provide the highest quality of healthcare. Our role includes the following:

- Contracts are in place with local health service providers;
- routine and emergency NHS services are available to patients;
- those services provide high quality care and value for money;
- paying those services for the care and treatment they have provided; and
- performance monitoring of commissioned services.

More detail can be found on our website at:
http://www.boltonccg.nhs.uk/about-us

Accurate, timely and relevant information is essential for our work. This helps us to design and plan current and future health and care services, evidence and review our decisions and manage budgets.

We also have a performance monitoring role of these services, which includes responding to any concerns or complaints (or if appropriate referring you to NHS England) for our patients regarding the services we offer.

Definitions of data types processed at the CCG

We use the following types of information / data:

Personal Data

This contains details that identify individuals even from one data item or a combination of data items. The following are demographic data items that are considered identifiable such as name, address, NHS Number, full postcode, date of birth. Under GDPR, this now includes location data and online identifiers.

Special Categories of Personal Data (previously known as Sensitive Data)

This is personal data consisting of information as to: race, ethnic origin, political opinions, health, religious beliefs, trade union membership, sexual life and previous criminal convictions. Under GDPR, this now includes biometric data and genetic data.

Personal Confidential Data

This term came from the Caldicott review undertaken in 2013 and describes personal information about identified or identifiable individuals, which should be kept private or secret. It includes personal data and special categories of data but it is adapted to include dead as well as living people and ‘confidential’ includes both information ‘given in confidence’ and ‘that which is owed a duty of confidence’.

Pseudonymised Data or Coded Data

Individual-level information where individuals can be distinguished by using a coded reference, which does not reveal their 'real world' identity. When data has been pseudonymised it still retains a level of detail in the replaced data by use of a key / code or pseudonym that should allow tracking back of the data to its original state.

Anonymised Data

This is data about individuals but with all identifying details removed. Data can be considered anonymised when it does not allow identification of the individuals to whom it relates, and it is not possible that any individual could be identified from the data by any further processing of that data or by processing it together with other information which is available or likely to be available.

Aggregated Data

This is statistical information about multiple individuals that has been combined to show general trends or values without identifying individuals within the data.

The CCG receives the following datasets from providers:

Primary Care Data

As many people's first point of contact with the NHS, around 90 per cent of patient interaction is with primary care services. In addition to GP practices, primary care covers dental practices, community pharmacies and high street optometrists. Primary Care Data relates to information which has been sourced from these types of services.

Secondary Care Data

Secondary Care means treatment and care of a specialised medical service by clinicians, for example, specialist doctors and nurses, within a health facility or hospital on referral by a primary care clinician such as your GP. Secondary Care data relates to information which has been sourced from these types of services.

Secondary Uses Service (SUS) Data

The Secondary Uses Service (SUS) is the single, comprehensive repository for healthcare data in England which enables a range of reporting and analyses to support the NHS in the delivery of healthcare services. When a patient or service user is treated or cared for, information is collected which supports their treatment. SUS data is useful to commissioners and providers of NHS-funded care for 'secondary' purposes – this is use of data other than for direct or 'primary' clinical care.

For further information about SUS, please visit:
https://digital.nhs.uk/services/secondary-uses-service-sus

Community Care / Social Care Data

Community care data includes data from social care services covering both adults and children.

Data Controller

A Data Controller determines the purposes and means of processing personal data. The CCG are a Data Controller.

Data Processor

A Data Processor acts on instruction by a Data Controller and processes data on behalf of the controller.

Our data processing activities

The law on data protection under the GDPR sets out a number of different reasons for which personal data can be processed. The law states that we have to inform you what the legal basis is for processing personal data and also if we process special category of data such as health data what the condition is for processing.

The types of processing we carry out in the CCG and the legal basis and conditions we use to do this are outlined below:

NHS Continuing Healthcare (CHC) applications

Type of data	Personal Data – Demographics Special category of data – Health Data
Source of Data	Primary Care and Secondary Care
Legal basis for processing Personal Data and Special Category of data under GDPR	Article 6 (1)(e) - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority Article 9(2)(h) - Processing is necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health and social care systems
Common Law Duty of Confidentiality basis	Implied Consent

If you make an application for NHS Continuing Healthcare (CHC) funding we will use the information you provide and where needed request further information from care providers to identify eligibility for funding. If agreed, arrangements will be put in place to provide and pay for the agreed funding packages with appointed care providers.

This process is nationally defined; we follow a standard process and use standard information collection tools when assessing eligibility for CHC applications.

NHS Continuing Healthcare (CHC) Verifying Patients

Type of data	Personal Data – Demographics Special category of data – Health Data
Source of Data	Primary Care and Secondary Care and Social Care
Legal basis for processing Personal Data and Special Category of data under GDPR	Article 6 (1)(e) - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority Article 9(2)(h) - Processing is necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health and social care systems
Common Law Duty of Confidentiality basis	Implied Consent

If you require services from the Continuing Healthcare team, the CCG need to ensure that you are registered at one of our GP Practices. We need to establish whether we are the responsible commissioner. Any delay in establishing who is responsible could lead to a delay in commissioning a care package or a placement in nursing care. This is particularly relevant in patients that have been referred to CHC under the fast-track criteria on the basis that they require immediate access to a package of care as they are nearing end of life.

In addition when one of our patients has passed away the Continuing Healthcare team need to be verify the date of the death. This will ensure that the team do not send letters / information to any patient (or next of kin) who has passed away. We understand this would cause upset and distress for families. As this information relates to people who have passed away this is not covered under the Data Protection Act 2018 or GDPR (only relates to living individuals). This means that no legal basis can be applied for this and the CCG would therefore allow access to prevent or reduce the risk of reputational damage and distress to relatives.

Individual Funding Requests

Type of data	Personal Data – demographics Special category of data – Health data
Source of Data	Primary and Secondary Care
Legal basis for processing Personal Data and Special Category of data under GDPR	Article 6 (1)(e) - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority Article 9(2)(h) - Processing is necessary for the purposes of preventative or occupational medicine for the assessment of the

	working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health and social care systems
Common Law Duty of Confidentiality basis	Implied Consent

You or your doctor on your behalf can make an Individual Funding Request (IFR) for a treatment not routinely commissioned. We use the information you provide and if necessary request further information from primary care and secondary care providers to identify eligibility for funding. This process is carried out by a data processor who acts on our behalf. The Data Processor for this purpose is Greater Manchester Shared Services - Effective Use of Resources Team. Please note this does not include IFR's for mental health, these are processed by the CCG directly.

For further information about Individual Funding Requests processed by the GMSS EUR, please click on the following link:

https://www.boltonccg.nhs.uk/how-we-do-things/effective-use-of-resources

Safeguarding

Type of data	Personal Data – Demographics Special category of data – Health Data
Source of Data	Primary Care, Secondary Care and Community Care
Legal basis for processing Personal Data and Special Category of data under GDPR	Article 6 (1)(e) - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority Article 9 (2)(b) - Processing is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or the data subject in the field of …social protection law
Common Law Duty of Confidentiality basis	Overriding Public Interest / Statutory legalisation for adult and children safeguarding

Information is provided to care providers to ensure that adult and children's safeguarding matters are managed appropriately. Access to personal confidential data will be shared in some limited circumstances where it's legally required for the safety of the individuals concerned.

For the purposes of safeguarding children and vulnerable adults, personal and healthcare data is disclosed under the provisions of the Children Acts 1989 and 2006 and Care Act 2014.

Incident Management – Serious Incidents

Type of data	Personal Data – demographics Special category of data – Health data
Source of Data	Primary Care, Secondary Care and Community Care

Legal basis for processing Personal Data and Special Category of data under GDPR	Article 6 (1)(e) - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority Article 9(2)(h) - Processing is necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health and social care systems
Common Law Duty of Confidentiality basis	Statutory – Serious Incident Framework 2015

Bolton CCG is accountable for effective governance and learning following all Serious Incidents (SI's). We work closely with all provider organisations as well as commissioning staff members to ensure all SI's are reported and managed appropriately.

The Francis Report (February 2013) emphasised that commissioners should have a primary responsibility for ensuring quality, as well as providers.

Supporting Medicines Optimisation

Type of data	Personal Data – demographics Special category of data – Health data
Source of Data	Primary Care
Legal basis for processing Personal Data and Special Category of data under GDPR	Article 6 (1)(e) - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority Article 9 (2)(h) - Processing is necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health and social care systems
Common Law Duty of Confidentiality basis	Implied Consent

The Medicines Optimisation Team work with GP practices to provide advice on medicines / prescribing queries and review prescribing of medicines to ensure that it is safe. In some cases, to ensure clinical safety, this may require the use of personal confidential data.

In cases where personal confidential data is required, this is done with the practice agreement. No data is removed from the practice's clinical system and no changes are made to patient's records without permission from the GP. Patient records may sometimes be viewed remotely via secure encrypted laptops from the CCG's premises. This is undertaken via a system called Bomgar.

Where specialist support is required, for example, to advise community pharmacists to order a drug that comes in solid form, in gas or liquid form; Bolton CCG medicines optimisation pharmacists will provide advice on behalf of a GP to support your care. Personal confidential data is used for this purpose.

Personal confidential data is also used by our medicines optimisation team to review and authorise (if appropriate) requests for high cost drugs which are not routinely funded. In cases where personal confidential data is used, this is done with permission from the GP.

Business Intelligence

Type of data	Personal Data – demographics Special category of data – Health data
Source of Data	Primary Care and Secondary Care
Legal basis for processing Personal Data and Special Category of data under GDPR	Article 6 (1)(e) - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority Article 9 (2)(h) - Processing is necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health and social care systems
Common Law Duty of Confidentiality basis	Implied Consent

The Business Intelligence team help our GP Practices in finding out which of their patients attended Bolton NHS Foundation Trust A&E or BARDOC Out of hours and who has been admitted or discharged (from Bolton NHS Foundation Trust) from the day before. This information is for direct patient care and is similar to the discharge letters that you will receive as a patient (but not as detailed) and that your GP Practice receives too. It enables our GP Practices to proactively contact any patients who have had hospital or Out Of Hours contact. Our GP Practices access this information electronically.

The Business Intelligence team ensure our GP Practices have the means to access this information. Please note that during this process the team do not view any patient information.

Secondary use of Data

Secondary use of data in the NHS is when patient data is not used for direct care but for other secondary purposes such as commissioning, risk stratification, financial and national clinical audit, healthcare management and planning, research and public health surveillance.

Disclosure of anonymised, pseudonymised or aggregated data (see section 'Definitions of data types processed at the CCG' for more information) will often satisfy a number of secondary uses and must be used in preference to patient / personal confidential data. Consent for disclosure of effectively de-identified data is not required. De-identification / pseudonymisation processes must occur before data leaves the source organisation. If a request is for identifiable data and the source organisation feels that de-identified data would suffice clarification should be obtained as to why identifiable data is required other than, exceptionally, where mandated by law such as under a Section 251 approval as per the NHS Act 2006 (see section below) or patient consent is obtained. Patients have the right to dissent from the disclosure of their personal confidential data for secondary purposes unless the law compels disclosure.

Section 251 of the NHS Act 2006

Section 251 of the NHS Act 2006 provides a mechanism which can enable the use of confidential information for certain purposes where it is unreasonable for consent to be obtained or that would otherwise be unlawful (e.g. information from NHS Digital on commissioning, Risk Stratification and Invoice Validation) through an application made to the Confidentiality Advisory Group (CAG).

The CAG assesses applications against the Health Service (Control of Patient Information) Regulations 2002 and provides independent expert advice to the Health Research Authority (HRA) and the Secretary of State for Health on whether an application to process patient information without consent should be approved.

The use of data for which an application is made must be for a medical purpose as defined in section 251 (12) of the NHS Act 2006.. This includes medical research and management of health and social care services.

Further information can be found on the Health Research Authority website – see the Links section below.

NHS Digital / Data Services for Commissioners Regional Office (DSCRO)

The law provides some NHS bodies, particularly NHS Digital, ways of collecting sensitive personal data directly from care providers for secondary purposes, such as evaluating care provided at population level.

NHS Digital is the national information and technology partner for the health and care system. The NHS Digital systems and information help doctors, nurses and other health care professionals improve efficiency and make care safer. We:

- provide information and data to the health service so that it can plan effectively and monitor progress
- create and maintain the technological infrastructure that keeps the health service running and links systems together to provide seamless care
- develop information standards that improve the way different parts of the system communicate

They are able to disseminate data to commissioners under the Health and Social Care Act (2012). The act provides the powers for NHS Digital to collect, analyse and disseminate national data and statistical information. To access this data, organisations must submit an application and demonstrate that they meet the appropriate governance and security requirements which the CCG has completed.

NHS Digital, through its Data Services for Commissioners Regional Offices (DSCROs), is permitted to collect, hold and process Personal Confidential Data (PCD). This is for purposes beyond direct patient care (secondary use) to support NHS commissioning organisations and the commissioning functions within local authorities

Data regarding health care treatment can only be shared with commissioning organisations where a formal Data Sharing Framework Contract (DSFC) is in place alongside a Data Sharing Agreement (DSA). These place a clear obligation on the receiving organisation to only use the supplied information for the agreed purposes. This data cannot be shared with others unless specified within the DSA.

Data may be linked by these special bodies so that it can be used to improve health care and development, and monitor NHS performance. In some cases there may also be a need to link local datasets, which could include a range of acute-based services such as radiology, physiotherapy and audiology, as well as mental health and community-based services such as Improving Access to Psychological Therapies (IAPT), district nursing and podiatry.

There is a data sharing agreement with DSCRO and the following CCG's to provide assurance regarding the security processes for pseudonymisation and for sharing such data as part of collaborative working with the following CCG's in Greater Manchester:

- NHS Bury Clinical Commissioning Group
- NHS Oldham Clinical Commissioning Group
- NHS Manchester Clinical Commissioning Group
- NHS Stockport Clinical Commissioning Group
- NHS Trafford Clinical Commissioning Group
- NHS Tameside & Glossop Clinical Commissioning Group
- NHS Wigan Clinical Commissioning Group
- NHS Salford CCG
- NHS Heywood, Middleton and Rochdale CCG

The dataset collected from secondary care providers, for example hospitals, by NHS Digital is referred to the Secondary Uses Service (SUS) is the single, comprehensive repository for healthcare data in England which enables a range of reporting and analyses to support the NHS in the delivery of healthcare services. When a patient or service user is treated or cared for, information is collected which supports their treatment. For further information, please visit NHS Digital's website: https://digital.nhs.uk/services/secondary-uses-service-sus

The following are the types of organisations NHS Digital receives data from, and then forwards on to our data processor in an anonymised format or a de-identified format with NHS Number in order to link and analyse the data.

Where data is used for these statistical purposes, stringent measures are taken to ensure individuals cannot be identified.

Types of organisations and types of information we receive:

- Acute Trusts – Hospitals [Bolton NHS Foundation Trust] - we receive anonymised acute data such as A&E attendances, waiting times, diagnosis, treatments, and follow ups, length of stay, discharge information and next steps.
- Community trusts or community organisations - we receive anonymised community data such as outpatient information, waiting times, diagnosis and treatments, referrals and next steps, domiciliary and district nursing (which includes home visits) and community rehabilitation units.
- Mental Health Trusts or Mental Health organisations [Greater Manchester Mental Health NHS Foundation Trust] - we receive anonymised mental health data such as rehabilitation and outpatient attendances, waiting times, diagnosis, treatment, length of stay, discharge, referrals and next steps.
- Primary Care organisations, for example your local GP practice. We receive anonymised primary care data such as attendances, diagnosis, treatment, GP or GP practice visits, referrals, medication/prescriptions information and follow-ups.

We may also contract with other organisations to process this data. We ensure external data processors that support us are legally and contractually bound to operate this process. They have security arrangements to maintain confidentiality where data that could or does identify a person is processed. The external data processors we work with to do this is NHS Arden and GEM Commissioning Support Unit (CSU).

The types of secondary use processing we do in the CCG are:

Risk Stratification

Type of data	Pseudonymised / Anonymised / Aggregate Data
Source of Data	Primary Care, Secondary Care and Community Care
Legal basis for processing Personal Data and Special Category of data under GDPR	Article 6 (1)(c) - Processing is necessary for compliance with a legal obligation Article 9(2)(h) - Processing is necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health and social care systems Section 251 NHS Act 2006

NHS England encourages CCGs and GPs to use risk stratification tools as part of their local strategies for supporting patients with long-term conditions and to help and prevent avoidable admissions. Knowledge of the risk profile of our population will help the CCG to commission appropriate preventative services and to promote quality improvement in collaboration with our GP practices.

Risk stratification tools use various combinations of historic information about patients, for example, age, gender, diagnoses and patterns of hospital attendance and admission and primary care data collected in GP practice systems.

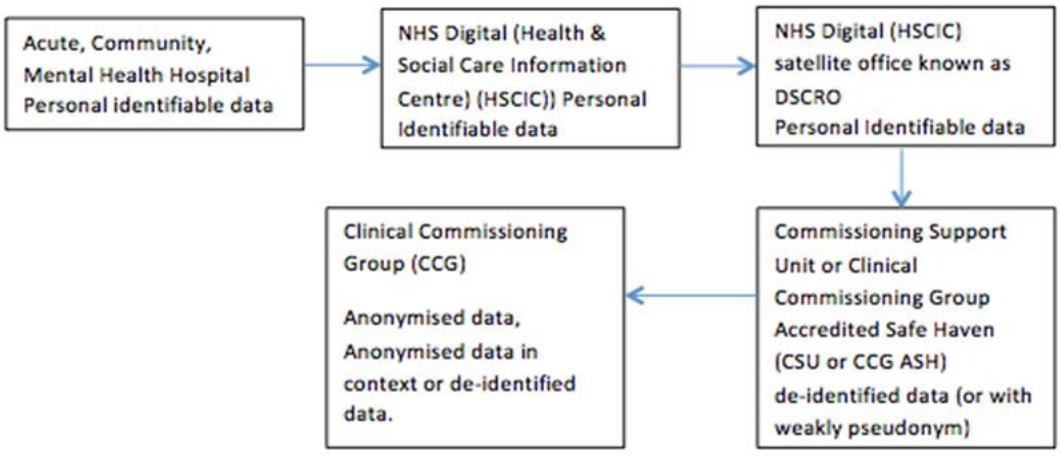
Risk stratification is a process which applies computer based algorithms, or calculations to identify those patients who are most at risk from certain medical conditions and who will benefit from clinical care to help prevent or better treat their condition. To identify those patients individually from the patient community would be a lengthy and time-consuming process which would by its nature potentially not identify individuals quickly and increase the time to improve care. A GP / health professional at your GP Practice will need to review this information before a decision is made.

There are two types of risk stratification:

- **Risk Stratification for case-finding** identifies/ manages patients who are at high risk of emergency hospital admission or to reduce the risk of certain diseases developing. This is called Risk Stratification for case-finding.

- **Risk Stratification for Commissioning** allows the CCG to understand the health needs of the local population in order to plan and commission the right services.

For risk stratification, there is a Section 251 approval in place which allows NHS Digital to receive personal confidential data. They process this via DSCRO who then send pseudonymised data to the CCG. This is detailed in the flow chart below.



The CCG also use a system / tool called Tableau to undertake anonymous / pseudonymised analysis.

If you do not wish information about you to be included in our risk stratification programme, please contact your GP Practice. They can add a code to your records that will stop your information from being used for this purpose.

Invoice Validation

Type of data	Personal Data – demographics Pseudonymised – coded health care data
Source of Data	GP Practice and other care providers
Legal basis for processing Personal Data and Special Category of data under GDPR	Article 6 (1)(c) - Processing is necessary for compliance with a legal obligation Article 9(2)(h) - Processing is necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health and social care systems Section 251 NHS Act 2006, NHS Constitution (Health and Social Care Act 2012)

There may be times where one healthcare organisation will need to invoice another for treatment given to a patient. This can occur, for example, when you need hospital treatment while away from home on holiday. The hospital at which you were seen may need to invoice us for the treatment you received.

Before paying the invoice, we will need to be sure that we, and not another CCG, are responsible for your treatment costs as well as checking to ensure that the amount the CCG are being billed for is correct. A limited amount of information about you needs to be processed Information such as your NHS Number and details of treatment. This information may be passed on to enable the billing process to proceed. This process is known as invoice validation.

These details are held in a secure environment and kept confidential. This information will only be used to validate invoices, and will not be shared for any further commissioning purposes.

Bolton CCG are registered as a Controlled Environment for Finance (CEfF) under a Section 251 exemption, this enables us to process patient identifiable information without consent for the purposes of invoice validation – CAG 7-07(a)(b)(c)/2013. In these cases we only use your NHS Number (no other identifiable information). Access is restricted to a small number of trained staff and can be audited if necessary.

NHS Shared Business Services – Finance and Accounting Services

Some provider invoices for patient care submitted to Clinical Commissioning Groups for payment are processed via NHS Shared Business Services. They provide support services for the NHS, providing finance and accounting solutions. NHS SBS also use offshore service provider called Sopra Steria who are based in India. Both NHS SBS and Sopra Steria have met the necessary information governance standards to process data overseas.

Purposes where consent is required

There are also other areas of processing undertaken where consent is required from you. Under GDPR, consent must be freely given, specific, you must be informed and a record must be made that you have given your consent, to confirm you have understood.

Patient and public involvement

Type of data	Personal Data – demographics
Source of Data	Data Subject
Legal basis for processing Personal Data under GDPR	Article 6 (1)(a) – Explicit Consent

If you have asked us to keep you regularly informed and up to date about the work of the CCG or if you are actively involved in our engagement and consultation activities or patient participation groups, we will collect and process personal confidential data which you consent to and share with us.

Where you submit or publish your details to us for involvement purposes, we will only use your information for this purpose and only with your written consent. You can contact us at any point to withdraw your consent for us to use your photograph, film and words for any new purposes.

Please remember that once an article is published and in circulation it may be copied and used by others (especially online). If you ask us to stop using your photo, film or words in the future we will comply with your request, but we cannot guarantee that other parties will do so.

To opt out of receiving updates or to withdraw your consent please contacting us at- Bolccg.communications@nhs.net.

Right of Access Requests (also known as Subject Access Requests)

Type of data	Personal Data – demographics
Source of Data	Data Subject
Legal basis for processing Personal Data under GDPR	Article 6 (1)(a) – Explicit Consent

If you have asked us for a copy of your data we will need your explicit, written consent (or your legal representative) before we proceed.

Incidents (non-serious) relating to CCG commissioned services

Type of data	Personal Data – demographics
Source of Data	Primary Care
Legal basis for processing Personal Data and Special Category of data under GDPR	Article 6 (1)(a) – Explicit Consent

The Governance and Risk Team work with providers such as GP Practices, Trusts, Care Homes etc to investigate non serious incidents. In the majority of cases personal confidential data is not required. However, in some cases to ensure the incident is investigated thoroughly this may require the use of personal confidential data. This information is limited and is restricted to the NHS Number only.

In cases where PCD (NHS Number) is required, the practice will obtain the explicit consent from the patient involved.

Complaints relating to the CCG

Type of data	Personal Data – demographics
Source of Data	Data Subject
Legal basis for processing Personal Data under GDPR	Article 6 (1)(a) – Explicit Consent

You can contact the Complaints team at: bolccg.complaints@nhs.net

Complaints relating to CCG commissioned services

Type of data	Personal Data – demographics Special category of data – Health data
Source of Data	Data Subject, Primary Care and Secondary Care and Community Care
Legal basis for processing Personal Data and Special Category of data under GDPR	Article 6 (1)(a) – Explicit Consent Article 9 (2)(h) - Processing is necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health and social care systems Common law duty of confidentiality – explicit consent

When we receive a complaint from a person about a commissioned service, we hold information about the complaint in our electronic files. This normally includes the identity of the complainant and any other individuals involved in the complaint. It may include special category data about individuals' heath care.

We usually have to disclose the complainant's identity to whoever the complaint is about. This is inevitable where, for example, the accuracy of a person's record is in dispute. If a complainant doesn't want information identifying him or her to be disclosed, we will try to respect that. However, it may not be possible to handle a complaint on an anonymous basis.

Before we proceed with handling a complaint we will obtain the explicit, written consent of the patient involved. We ensure they are aware of how and with whom their data may be shared by us, including if they have a representative they wish us to deal with on their behalf.

For more information please contact:

NHS Bolton Clinical Commissioning Group
PALS and Complaints Team
St Peter's House
Silverwell Street
Bolton
BL1 1PP

Email: bolcgg.complaints@nhs.net

Other Partner Organisations

We contract with other organisations (as listed in the table below) who provide us with additional expertise to support the work of the CCG. On some occasions, they may access personal data, for example, IT Services may have to access computer systems to fix a fault. We ensure the external data processors that support us are legally and contractually bound to operate this process via contracts / Information Sharing Agreements. These re-inforce their responsibilities as a data processor to ensure your data is securely protected.

These are the current external data processors we work with who provide a service:

Purpose	Data Processor
To provide the following: Effective Use of Resources / IT Services	NHS Greater Manchester Shared Services (GMSS) Ellen House Waddington Street Oldham OL9 6EE
To provide the following: Human Resources and Payroll Services	Bolton NHS Foundation Trust Minerva Rd, Farnworth, Bolton BL4 0JR

Using anonymous or aggregate information

This type of data is used to help assess the needs of the general population and / or in the area and surrounding areas of Bolton. This helps us make informed decisions and prepare reports on the services we commission to assess:

- The quality and efficiency of the health services we commission;
- To work out what illnesses people will have in the future, so we can plan and prioritise services and ensure these meet the needs of patients in the future; and
- To review the care being provided to make sure it is of the highest standard.

Where information is used for statistical purposes, secure measures are taken to ensure individuals cannot be identified. Anonymous information may also be passed to neighbouring CCG's and councils as part of integrated working.

How we protect your personal data

We are committed to protecting your privacy and will only process personal data in accordance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018, the Common Law Duty of Confidentiality and the Human Rights Act 1998.

All information is subject to rigorous measures and procedures to make sure it cannot be seen, accessed or disclosed to any inappropriate persons. We have an Information Governance Framework that explains the data security governance within the CCG.

Access to electronic data is password protected on secure network and / or online systems and paper documentation is filed securely in lockable storage cabinets.

Our IT Services provider, Greater Manchester Shared Services, regularly monitor our system for potential vulnerabilities and attacks and look to always ensure security is strengthened.

Everyone working for the NHS has a legal duty to keep information about you confidential and comply with the common law duty of confidentiality and other NHS guidance.

All of our staff including contractors and committee members receive appropriate and on-going data security training to ensure they are aware of their personal responsibilities and have contractual obligations to uphold confidentiality, enforceable through disciplinary procedures.

We have incident reporting and management processes in place for reporting any data breaches or incidents. We learn from such events to help prevent further issues and inform data subjects of breaches when required.

Every NHS organisation has a senior person that is responsible for information risk and security of information. This person is known as the Senior Information Risk Owner (SIRO), and within the CCG, this role is assigned to:

Ian Boyle, Chief Finance Officer

The CCG also has a nominate Data Protection Officer (DPO). A Data Protection Officer is a senior role who is responsible for advising colleagues on compliance, training and awareness raising, monitoring compliance and carrying out audits. The DPO is the main point of contact with the Information Commissioners Office (ICO).

The DPO for the CCG is:

Michael Robinson, Associate Director for Governance and Safety

How long do we keep your personal data (Retention and Destruction?

Retention

Whenever we collect or process your data, we will only keep it for as long as is necessary for the purpose it was collected. In the NHS, all commissioners and providers apply retention schedules in accordance with the Records Management Code of Practice for Health and Social Care (refer to Link section below). This code is based on current legal requirements and professional best practice and sets the required standard of practice in the management of records for those who work within or contract to NHS organisations in England.

Destruction

Destruction of data will only happen following a "review" of the information at the end of its retention period. Where data has been identified for disposal we have the following responsibilities:

- To ensure that information held in manual form (regardless of whether originally or printed from the IT systems) is destroyed using a cross cut shredder or subcontracted to a reputable confidential waste company (as identified in the table below) that complies with European Standard EN15713.
- To ensure that electronic storage media used to hold or process information are destroyed or overwritten to current national cyber security standards.
- To ensure that any arrangement made to sub-contract secure disposal services from another provider, complies with the NHS Standard Contract and with assurance that the sub-contractor's organisational and technical security measures comply with the General Data Protection Regulations (GDPR) and the Data Protection Act 2018.

Who we share your data with?

We share information that does not identify you (anonymised) with other NHS and social care partner agencies for the purpose of improving local services, research, audit and public health.

We would not share information that identifies you unless you have given us permission (consent). However, there are certain circumstances where we will process / share personal information without your consent and where there is another legal statute or law allowing us to do this which are:

- To protect children and vulnerable adults
- When a formal court order has been served upon us; and / or
- When we are lawfully required to report certain information to the appropriate authorities e.g. to prevent fraud or a serious crime;

- Emergency Planning reasons such as for protecting the health and safety of others;
- When permission is given by the Secretary of State or the Health Research Authority on the advice of the Confidentiality Advisory Group to process confidential information without the explicit consent of individuals (see section on Section 251 of the NHS Act 2006).

When analysing current health services and proposals for developing future services, it is sometimes necessary to link separate individual datasets to be able to produce a comprehensive evaluation. This may involve linking primary care GP data with secondary uses service (SUS) data (inpatient, outpatient and A&E).

In some cases, there may also be a need to link local datasets, which could include a range of acute-based services such as radiology, physiotherapy and audiology, as well as mental health and community-based services such as district nursing and podiatry. When carrying out this analysis, the linking of these datasets is always done using a pseudonym. This means that the data is coded and individuals are not identifiable.

Where is your data processed?

Your data is processed within the CCG and by other third parties as stated above who are UK based.

Processing outside of the UK

As detailed in the invoice validation section, NHS Shared Business Services use an offshore service provider called Sopra Steria who is based in India. NHS SBS have confirmed that Sopra Steria have met the necessary information governance standards to process data overseas.

We will not disclose any health information without an appropriate lawful principle, unless there are exceptional circumstances such as when the health or safety of others is at risk, where the law requires it, or to carry out a statutory functions i.e. reporting to external bodies to meet legal obligations.

What are your rights over your personal data?

You have a number of rights over your data under the Data Protection Act 2018 and General Data Protection Regulation 2018 (GDPR):

- Right to be Informed
- Right of Access
- Right to Rectification
- Right to Erasure
- Right to Data Portability
- Right not to be subject to a decision based solely on automated processing

- Right to withdraw consent
- Right to object to processing
- Right to restriction of processing

Right to be Informed

You have a right to be informed about uses of your information with an emphasis on transparency. This notice, in support of other privacy notices published by the CCG, ensures that your right to be informed is achieved.

Right of Access

You are entitled to request to view / ask for a copy of the information the CCG hold about you this is known as a Right of Access request but can also be referred to as a Subject Access Request (SAR). We request that you provide this in writing / email to us with identification and provide adequate information to help us process your request. If we need further information, we will ask you to provide this.

There is no charge (subject to exemptions) to have a copy of the information held about you and we must respond to you within one calendar month (subject to exemptions).

To request a copy of or request access to information we hold about you and / or to request information to be corrected if it is inaccurate, please contact:

Bolton CCG Right of Access Lead at:
NHS Bolton CCG, St Peters House, Silverwell Street, Bolton, BL1 1PP
Or Email: bolccg.quality-team@nhs.net

Requests are handled in line with our Right of Access / Subject Access Requests Procedure which can be found on the CCG's website. You can use the Right of Access Request form within the procedure to make your request, if you find this is helpful. To request a copy of this form please contact the Governance team at the email address as above or visit the procedure.

For any postal requests please ensure it is marked private and confidential and addressed to the CCG Right of Access Lead.

The CCG hold a limited amount of healthcare data as detailed above. To request access to GP records, please contact your GP practice and to request access to hospital records, please contact the hospital you attended for treatment / care.

You should also be aware that in certain circumstances, your right to see some details in your health records held by the CCG may be withheld. This may be because releasing the information could cause serious harm to your physical or mental health or if there is 3rd party information that cannot be released.

Right to Rectification

Rectification refers to correcting inaccuracies or incomplete data which is held by the CCG. This applies to factual information only – such as identifiers and next of kin. The CCG is unable to remove or alter professional opinions which you may disagree with. You do however; have the right to include your own statements alongside professional opinions.

The correction of personal data when incorrect, out of date or incomplete which must be acted upon within 1 calendar month of receipt of such request. Please ensure the CCG has the correct contact details for you.

Right to Erasure ('forgotten')

In some circumstances you can request that your information is deleted.

This right will apply if the processing has been undertaken on the basis of consent which is withdrawn, the processing of data is determined not to be lawful or the information is no longer required. You will be informed of activities to which this right applies.

Only if we have your explicit consent for any processing we do, you have the right to withdraw that consent at any time and have the right to request this data to be deleted / erased. Please note this will not apply where healthcare data is processed.

Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

Only if we have your explicit consent for any processing we do, and the CCG is able to, you have the right to have data provided to you in a format you have requested such as an excel spreadsheet, csv file.

Right not to be subject to a decision based solely on automated processing

Automated decision making is the use of computer systems or definitions to apply rules to data in order to determine an outcome – credit ratings are an example of automated decision making.

The CCG do not process data using this method, so this right will not apply to our data processing activities.

Right to withdraw consent

The legal basis to process your personal and special category of data generally, falls within Articles 6(1)(e) and 9(2)(b) and (h) of the GDPR. Other processing may be appropriate under Articles 6(1)(b), 6(1)(c), 6(1)(d) and 6(1)(f). Where these do not apply, any other processing will be reliant on your consent under Article 6(1)(a); this will be based on explicit consent under GDPR and as a result, you will be asked to

make a definite decision; there will be no presumption of consent from silence, inaction or pre-selected choices.

You have the right to refuse (or withdraw) consent to information sharing at any time. However, this may not be possible if the sharing is a mandatory or legal requirement imposed on the CCG. Any restrictions, and the possible consequences of withholding your consent, will be fully explained to you as the situation arises.

Right to object to processing

There is no general right to object to processing; however, you can object if there are grounds relating to your own particular situation, or if information is likely to be used for:

- Marketing
- Scientific or historical research
- Statistical purposes
- Purposes in the public interest or under an official authority (e.g. NHS Act 2006)

You have the right to object to processing. However please note if we can demonstrate compelling legitimate grounds which outweighs the interest of you then processing can continue. If we didn't process any information about you and your health care (where the CCG process health data) it would be very difficult for us to care and treat you.

Objections to processing for secondary care purposes

The NHS Constitution states that "You have the right to request that your confidential information is not used beyond your own care and treatment and to have your objections considered".

In line with this there are choices you can make about how your information is used, and you can choose to opt out of your information being shared or used for any purpose beyond providing your care. The National Data Opt-Out Policy is a new service that allows individuals to opt out of their confidential patient information being used for research and planning. It was introduced on 25 May 2018, providing a facility for individuals to opt-out from the use of their data for research or planning purposes. The CCG have reviewed the areas where they process personal data and can confirm they do not use personal data for any purpose other than Direct Patient Care. The CCG predominately processes non-identifiable data. Therefore, the National Data Opt-Out Policy does not apply to our CCG.

For further information on the National Data Opt-Out Policy and if you have any concerns about the data we process about you please contact the Information Governance Team at:

Email: Bolccg.communications@nhs.net

(Please note this email account is accessed by a number of personnel therefore consider the information provided when contacting and please state who the email is intended for)

Or you can use the "Contact Us" page on the Bolton CCG website at the link below:

https://www.boltonccg.nhs.uk/contact-us

Right to restriction of processing

This right enables individuals to suspend the processing of personal information, for example, you have disputed the accuracy of information, objected to its use or require data due for destruction to be maintained for a legal claim.

Complaints / Contacting the Regulator

If you feel that your personal data we hold at the CCG has not been handled correctly or you are unhappy with our response to any requests you have made to us regarding the use of personal data, please contact our Data Protection Officer (DPO) at the following contact details. Under GDPR all public bodies must nominate a Data Protection Officer. The DPO is responsible for advising on compliance, training and awareness is the main point of contact with the Information Commissioner.

DPO for Bolton CCG:

Michael Robinson
Email: michael.robinson1@nhs.net

Address: NHS Bolton CCG, St Peters House, Silverwell Street, Bolton, BL1 1PP

If you are not happy with our responses and believe we are not processing your personal data in accordance with the law you may wish to take your complaint to a supervisory authority, you have the right to lodge a complaint with the Information Commissioner's Office (ICO).

You can contact them by calling 0303 123 1133

Or go online www.ico.org.uk/concerns

Data Protection Registration

Any organisation that processes Personal Data whether they are a Data Controller or Data Processor is required to pay a data protection fee to the Information Commissioner's Office (ICO) annually. The ICO publish a register of all registered organisations. This can be found here: https://ico.org.uk/ESDWebPages/Search

Bolton CCG is a registered 'Data Controller' with the ICO.

ICO Registration Number: ZA007073
Date Registered: 13th June 2013
Registration Expires: 12th June 2020

Data Security and Protection Toolkit

The Data Security and Protection Toolkit is an online assessment that must be completed every year by organisations who process Personal Data.

It is based on the National Data Guardian 10 Data Security Standards and also incorporates key requirements of the Data Protection legislation.

It measures whether an organisation is Data Protection compliant. Organisations are asked to provide evidence to show how they meet each standard.

The final assessment and scores must be submitted by 31 March each year and are shared with the Care Quality Commission, Audit Commission and NHS England.

For the year 2018/19 the CCG submitted a successful Toolkit and achieved 'Standards Met.'

To provide additional assurance the CCG's Toolkit was audited in March 2019 by Mersey Internal Audit Agency and achieved 'Substantial Assurance.'

Further Information / Contact Us

We hope that this privacy notice has been helpful in setting out the way we handle your personal data at the CCG and your rights to control it. If you have any queries / or would like further information, please visit the useful websites below and / or contact us at the following contact details.

Address: NHS Bolton CCG, St Peters House, Silverwell Street, Bolton, BL1 1PP

Bolccg.communications@nhs.net

Phone: 01204 46 2000

Links

If you would like to find out more useful information on the wider health & care social system approach to using personal information, please see the links below:

- Information Commissioners Office (ICO)
- Information Governance Alliance

- NHS Constitution
- NHS Care Record Guarantee
- NHS Digital Guide to Confidentiality in Health and Social Care
- Health Research Authority
- Health Research Authority Confidentiality Advisory Group (CAG)
- NHS Digital
- Records Management Code of Practice for Health & Social Care
- Secondary Uses Service (SUS)