Privacy Notice for Patients, Carers and Service Users

Who is Bristol Community Health CIC

Bristol Community Health (BCH) is a community interest company (CIC) established in 2011. We are the leading provider for community healthcare in Bristol, with over 40 different services, ranging from community nursing teams and end of life care to prison healthcare, school nursing, health visiting, diabetes support and physiotherapy. As a social enterprise and CIC, we are subject to particular rules, which include, requiring us to apply any profit or surplus that we make during the year into community projects and improving services and supporting our staff.

Our clinicians make 35,000 adult and 1,500 children's healthcare 'contacts' every month and treat a third of Bristol's over 65s. Over the last year, we've prevented at least 4,000 adults from being admitted into acute care and supported over 3,200 to come home from hospital early.

Most of our services are provided under contracts with NHS commissioners in the community or in the home, helping people to live life well in the comfort of their own surroundings. By doing this, we also help prevent hospital admissions. We also welcome innovation which helps us to deliver better care – for example, all of our community nurses use mobile working, which reduces bureaucracy and frees up time to care.

Through a partnership called the Community Children's Health Partnership (CCHP) our staff work alongside those from Sirona Care & Health (the partnership's lead provider), Avon and Wiltshire Mental Health Partnership NHS Trust (AWP) and Barnardo's to provide child healthcare and child and adolescent mental healthcare across Bristol and South Gloucestershire. We are specifically responsible for the children's community health services within this partnership.

We provide Prison Healthcare Services through another partnership called InspireBetterHealth. Partner organisations include ourselves as the lead provider, Avon and Wiltshire Mental Health Partnership NHS Trust, Hanham Health, GP Care, Time for Teeth, Homecare Opticians, Day Lewis Pharmacy and Sirona Care & Health CIC.

This document relates to the personal data of:

- patients receiving direct health or social care from BCH staff, contracted or temporary staff (known from now on as 'staff');
- patients receiving health or social care from our partner organisations and our staff working together;
- research participants or potential participants.

Information is given at the end of this notice on who to contact at BCH if you would like to talk about data protection or get further support.

What is a privacy notice?

A privacy notice is a notice which communicates our commitment to ensuring that we process your personal information and any data we collect and hold about you fairly, lawfully, openly and responsibly. It is a statement by BCH describing how we 'process' your data, which means:

- What information we collect about you
- Who is collecting it
- Why the information is needed
- Sources of information we use
- Who may we share it with

It also tells you how your data is used, who is in charge of its management and what rights you have under Data Protection Law (see below) to ask questions about how we are using your personal data and what controls are in place in relation to how we use it. It explains your rights to:

- Access data, information and records should you want to see them or if you move abroad;
- Deal with mistakes or delete data that you believe to be wrongly entered or wrongly held;
- The circumstances under which requests to access data may be denied; and
- How you can make a complaint or comment if you are dissatisfied with any aspect of the management of your information and patient record.

We publish this notice widely as a legal duty to patients, service users, visitors, carers, the public and staff. It is sometimes also referred to as a Privacy Statement and summarises a number of policies, procedures and documents relating to our management and protection of Data, Confidentiality and Security. This is also known across the health service as Information Governance.

Why issue a privacy notice?

Everybody who works in Health and Social Care has a legal duty to keep information about patients, staff and service users confidential and secure. They must comply with Data Protection Law. From 25 May 2018 the processing of personal data by BCH and its partners will have to comply with a new European Law Regulation (EU) 2016/679, the General Data Protection Regulation, (GDPR) which comes into force on that date. This notice is one of the ways in which we can demonstrate our commitment to providing services that meet all applicable standards and our legal obligations under the GDPR and Data Protection Law generally as described below.

Data Protection Law

Data protection law means any applicable law relating to the processing, privacy and use of personal data. This includes the UK Data Protection Act 1998 and the GDPR and any laws which implement, replace, extend, re-enact, consolidate or amend any such laws. It also means all guidance, guidelines, codes of practice and codes of conduct issued by any relevant supervisory authority relating to such Data Protection Laws. (**Data Protection Law**) In the UK a new Data Protection Bill is currently going through Parliament which will result in a new Data Protection Act

2018 which will detail in full the legal grounds for collecting, using and retaining personal data and sensitive personal data and will include a range of conditions and safeguards that will apply in relation to the same.

There are a number of key definitions and principles which are used in Data Protection Law which apply in relation to us collecting, holding and processing the information on your patient record. We set these out below:

Definitions

'Anonymisation' – process of turning data into a form which does not identify individuals and where identification is not likely to take place.

'Confidential Patient Information' - information to which a duty of confidentiality is owed under common law. Personal data including any health related information (including where health related information can be derived from context) or health related information in a context from which personal data can be identified, would be confidential patient information.

'Consent' - any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

'**Data Controller'** means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are or are to be processed.

'**Data Processor'** means in relation to personal data any person (other than an employee of the Data Controller) who processes data on behalf of a Data Controller.

'Data Protection Authority' (DPA) – an independent public authority tasked to ensure GDPR compliance. This is the Information Commissioner's Office (*ICO*) in the UK.

'Data Protection Officer' (DPO) – an expert on data privacy who works independently within a business to ensure GDPR is being adhered to. Mandatory in certain circumstances.

'Data Subject' – a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

'GDPR' - refers to requirements in both the EU General Data Protection Regulation and the forthcoming UK Data Protection Act. Note that Article 4 of the regulations lists definitions for the terms used in new UK data protection law.

'**Personal Data'** - defined as in the above regulations means any information relating to an identified or identifiable natural person (known as a 'Data Subject').

'Personal Data Breach' – a breach of security leading to the accidental or unlawful destruction, loss,

alteration, un-authorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

'Pseudonymous Data' - information that no longer allows the identification of an individual without additional information and is kept separate from it. For example a name is replaced with a unique number. The purpose is to render the data record less easy to identify with the original person and therefore reduce concerns when sharing and keeping it. Note that personal data that has been pseudonymised can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

'Special Category Data' - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Principles

Data Protection Law also sets out the principles with which Data Controllers and Data Processors must comply when processing personal information. As a Data Controller we are required to comply with these principles, which state that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely by us including where we share it with third parties.
- Made accessible to you and communicated to you how to exercise your rights in relation to it.

Why and how we collect information and the type of information we collect

We may ask for, or hold, 'confidential patient information' about you which will be used to support delivery of appropriate, safe and effective care and treatment. We need to be able to process such data (referred to as 'data processing') in all the locations where we provide care to you – whether that is in your home, or in local surgeries and clinics, in secure settings or in office locations.

The confidential patient information (and records of this information) about you, which we collect hold and use may include personal data such as:

- Name, address, date of birth, next of kin.
- Contact we have had over time with you, such as appointments and home visits.
- Details and notes about treatment and care, including notes and reports about your health.
- Results of x-rays, blood tests, etc.
- Information from people who care for you and know you well, such as health professionals and relatives.

It may also include more sensitive information (defined in the GDPR as 'Special Category' Data) such as details relating to your sexuality, race, your religion or beliefs, and whether you have a disability, allergies or health conditions. It is important for us to have a complete picture, as this information assists staff involved in your care to deliver appropriate treatment and care plans and to provide improved care, to meet your needs.

Information is collected in a number of ways, but here are some of the most commonly used:

- verbally when you are with your healthcare professional;
- manually when you fill in referral, assessment and other forms;
- via electronic or postal communications or records completed by a nurse, GP, administrator, pharmacist, specialist unit consultant or hospital-based staff and clinicians;
- directly given by social services, carers, relatives and friends over the phone or in person;
- in emergency situations by the social services, police or ambulance service staff.

Although we do not currently process your data in this way, in the future it would be important to tell you in detail about:

- the automatic tracking of people or their location online or by smart devices (for example, when we use automatic monitoring devices);
- the combining of different types of data (such as the use of satellite navigation data with other data); or
- using algorithms to analyse a variety of data, such as social media, location data and records in order to profile people for example in terms of their state of health or suitability for a particular treatment.

How we use information

- To help inform decisions that we make about your care.
- To ensure that your treatment is safe and effective.
- To work effectively with other organisations who may be involved in your care.
- To support the health of the general public.
- To ensure our services can meet future needs.
- To review care provided to ensure it is of the highest standard possible.
- To train healthcare professionals.
- For research and audit.
- To prepare statistics on BCH and NHS performance.
- To monitor how we spend public money.

We may also need to use or share your information under our contract to help the whole NHS to deliver care and improve health and care services. The information can be used to help:

- Improve individual care.
- Understand more about disease risks and causes.
- Improve diagnosis.
- Develop new treatments and prevent disease.
- Plan services.
- Improve patient safety.

- National programmes for audit and quality improvement.
- Inform Government, NHS and Social Care policy.

This is of potential benefit to you and all users of BCH and NHS services because:

1. Accurate and up-to-date information assists us to provide the best possible care and
2. Other healthcare professionals, specialists or staff working in other departments providing services funded by the NHS, can readily access information they need to provide care to patients without having to ask for the same information again.

However, where possible, when using information to inform future service and healthcare provision, non-identifiable information will be used.

If you have any questions about how we are collecting and using your data, please don't hesitate to ask our staff or contact our Data Protection Officer, details of which are set out at the end of this privacy notice.

Legal Basis for Holding and Processing Personal Data

All patient data is held by BCH staff under a common law "duty of confidence" and we work on the principle that personal data is only collected when needed for us to provide your care. Wherever possible, however, data is pseudonymised or anonymised.

BCH will only use personal data and so-called "special category" data in a way permitted by the law and this means that as from 25 May 2018 we will only process patient data and your data in accordance with GDPR, common law and the lawful bases set out in UK Data Protection Law. Processing personal data is deemed legal as defined in Article 6 of the GDPR, so long as at least one of the following applies:

1. purposes of the legitimate interests pursued by the organisation or by a third party, *except* where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of their Personal Data, in particular where the Data Subject is a child;
2. to protect the vital interests of the Data Subject or of another person;
3. to perform a task carried out in the public interest or in the exercise of official authority given to the organisation;
4. to comply with legal requirements for the discharge of an organisation's tasks or functions;
5. because the processing is necessary for the purposes of a contract with the individual [for example, the person has an employment contract with BCH];
6. the Data Subject has given Consent to the processing of his or her personal data for one or more specific purposes.

A SUMMARY OF THE LAWFUL BASES FOR PROCESSING PERSONAL DATA

This is a user friendly summary of Article 6 of the GDPR. Article 6 should be read in full if you want to know the law in detail.

At least one of these must apply whenever we process your Personal Data.

1. **Legitimate Interests:** the processing is necessary for our legitimate interests or the legitimate interests of a third party unless your rights and freedoms in relation to your Personal Data override those legitimate interests.
2. **Vital Interests:** the processing is necessary to protect someone's life.
3. **Public Task:** the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
4. **Legal Obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).
5. **Contract:** the processing is necessary for a contract we have with you, or because you have asked us to take specific steps before entering into a contract.
6. **Consent:** you have given clear consent for us to process your Personal Data for a specific purpose.

In relation to the provision of health and social care provided by BCH and our partners the following should be taken into account:

a. in all situations subject to the interests and fundamental rights and freedoms of the Data Subject regarding the protection of their Personal Data, the processing of Personal Data will be undertaken within **'legitimate interests'** and in (b) (c) or (d) below, additional legal bases apply;

b. for emergency or life threatening situations, the processing of Personal Data will be undertaken **'to protect the vital interest'** of the person or persons involved or if the Data Subject is physically or legally unable to give Consent as defined under the Mental Capacity Act (2005);

c. for research under contract with universities, NHS organisations or Research Council institutions, the processing of Personal Data will be a **'task in the public interest'**;

d. when required by '**legal obligation'** to an authority such as a coroner's court, security services or the police.

We have a legitimate interest in processing your personal data in order to provide you with the levels of individual assessment, diagnosis and treatment that enable our staff and the systems we use to deliver a responsive, caring, confidential and safe service. We are particularly mindful of protecting the personal data of children in our care. We are also required to demonstrate our performance under our contracts with NHS commissioners which we could not do if we did not collect information from everyone using our services. Finally, we are under legal obligations

connected with our registration as a health and social care provider to ensure that our services are responsive and effectively integrated with our partners. So, having carefully considered the new regulations, we have assessed that we could not achieve our purpose as a Social Enterprise without processing personal data from users. We are required under the new law to review this position with our information governance and legal advisers and report on a regular basis to check that our interests do not override those of our users.

In practice we will now only use 'Consent' as a basis for processing your Personal Data in specific situations where use of the information is within your choice and control and the processes involved are transparent (for example small scale one-off research or user involvement projects). In such circumstances, this would be with the full involvement of you and carried out under specific contracts with you that will give you all the detail on your rights.

Legal Basis for Holding and Processing Special Category Data

As stated above, Special Category Data is Personal Data which the GDPR says is more sensitive, and so needs more protection. There is a general prohibition on the processing of Special Category Data subject to a list of exceptions. The prohibition and exceptions are set out in Article 9 of the GDPR.

Special Category Data specifically includes genetic and biometric data – where processed for the purposes of providing a unique identifier for an individual. Information relating to criminal convictions and offences are now dealt with under separate provisions.

In accordance with Article 9 BCH can process Special Category Data (pursuant to one of the exceptions) where it is necessary for any of the purposes outlined in Article 9 (2) (h), for example, for, preventive or occupational medicine, for medical diagnosis or for the provision of health or social care or treatment or the management of health or social care systems and services, **but only on condition that:**

1. those purposes are fulfilled on the basis of UK law or because BCH enters into a contract with a health professional and

2. the data is processed by or under the responsibility of a professional subject to the obligation of professional secrecy under UK law or rules established by a national body (in the case of the UK the NHS).

As far as BCH is concerned because our services are provided in accordance with UK law and pursuant to contracts with the NHS which are under the responsibility of professionals who are subject to the obligation of professional secrecy as provided for by UK law and NHS rules we can process Special Category Data provided we continue to comply with the provisions of Article 9.

Our staff members are bound by legal, professional and contractual rules to ensure that they are qualified, trained and use competent and secure systems. In some circumstances for example, in relation to monitoring equality and diversity, we ensure that we have appropriate, specific policy documents which clearly outline the need for and the laws and rules which govern the processing of that data.

How information is stored and kept safe?

The laws and governance we have described also set out legally how we must store personal information including monitoring and managing the risk of 'breach' (for example data being lost or sent to a third party in error). Strict policy and procedures govern our use of your Personal Data and our duty to ensure it is kept safe and secure.

Information is retained in secure electronic and paper records on our information systems and accessed by staff through desktop, laptop and other mobile devices. Paper records are kept securely locked away when not in use, or held by the patient themselves and keyholders are strictly monitored. Such access is strictly restricted to staff provided with the equipment, passwords and other security devices we use to ensure that only those people who need to see your Personal Data in order to process it correctly can do so.

Ensuring that our staff and patients are aware of the importance of keeping personal records safe and secure at all times is also a key element of risk management around safety and security of record keeping. Staff sign up to their obligation of secrecy in their employment contracts and policies and procedures provide written, regularly updated guidance on our approach to storage and archiving Personal Data. This is backed up by training commencing with induction when members of staff arrive, ongoing update training and special training if required (e.g. for staff who archive records) and audit to make sure that policies and procedures are being followed correctly.

Bristol Community Health CIC is registered with the Information Commissioners Office (ICO). Details of our registration can be found on https://ico.org.uk/esdwebpages/search Follow this link and enter our registration number Z2842001 and click 'search the register' or just click on the number.

How do we keep information confidential?

The reason why Personal Data is kept safe and secure is to protect your privacy and confidentiality. There are a number of ways in which your privacy is shielded; by removing your identifying information, using an independent review process, adhering to strict contractual conditions, having up to date policies and procedures that all our staff are trained to follow, ensuring strict sharing or processing agreements are in place with our partners and auditing to make sure that staff are following the correct procedures.

Everyone working for BCH is made aware during their induction that they are subject to the Common Law Duty of Confidentiality, the GDPR and UK Data Protection Act (the Data Protection Laws) and our own Data Protection, IT Security and Information Governance policies and procedures.

All our staff are required to inform you, or people caring for you, of how the information they collect will be used, to explain the basis upon which we keep your data on our systems and share it where necessary. These conversations will be noted in your records and you have the right to view these if you wish to.

All staff are required to undertake annual training in data protection, confidentiality, IT/cyber security, with additional training for specialist staff such as those managing IT systems.

How long do we keep Personal Data?

Under Data Protection Law we must not keep any Personal Data for longer than we need to or process your data following your discharge from our service without explanation. Retaining records and archiving is covered in our Records Management Policy and Procedures which is followed by all relevant staff and departments.

Patient records are kept for the length of time that is required by the Government in its 'code of practice.' For more information, visit the NHS Choices website.

Will we share your information?

To provide best care possible information is shared between our staff member and between departments, but sometimes we will need to share information about you with others outside our organisation. We may need to share your information as part of our service to you with other health and social care organisation and regulatory bodies.

Connecting Care is the name given to a system we are using to share key parts of your health and care records for the purpose of providing a more coordinated service and improved quality of care. Connecting Care is a partnership of NHS health and social care organisations and the providers commissioned by them to deliver services and care to the residents of Bristol, North Somerset and South Gloucestershire. For all information about arrangements for sharing your personal information, please see https://www.connectingcarebnssg.co.uk/ and contact us if you have any questions.

Neither we, nor our partners can share or use any of your information unless it is necessary and in line with how you would reasonably expect the data to be used. Any sharing that takes place will always be in compliance with Data Protection Law. You may be contacted by any one of these organisations for a specific reason; they will have a duty to tell you why they have contacted you. Information sharing is governed by specific rules and law and recorded on the register with the Information Commissioner's Office.

Sharing with non-NHS organisations

So long as there is a lawful basis for us to do so in accordance with Data Protection Law, we may also need to share information from your records with non-NHS funded organisations, from whom you are also receiving care, such as care homes, agencies or other private healthcare organisations. However, we will not disclose any health information to third parties without your knowledge unless there are exceptional circumstances, such as when the health or safety of others is at risk or where the law requires the disclosure of information.

Other organisations may include, but are not restricted to: GPs; private sector hospital, specialist and community services, social care providers; education services; local authorities; the police, security services and prison authorities; voluntary sector and other private or voluntary sector

providers (e.g. health sector charities, dentists, podiatrists).

We may also be asked to share personal and special category data about you, which may include sensitive information from your health records. Generally, we would only do this to assist them to carry out their statutory duties.

Where patient information is shared with external organisations (other than through Connecting Care), an agreement is drawn up within the contract arrangements so that it is shared in a way that complies with Data Protection Law and meets information governance standards.

What happens if there is a Personal Data Breach and you are involved?

Any incidents involving loss of **Personal Data** will be reported as incidents on our systems. Not all such breaches will require further action, all will be investigated internally and what happens next is based on what data has been exposed and what risk that poses. If we discover that a breach is likely to result in a risk to your and other people's rights and freedoms or will adversely affect them, we will inform you under our Duty of Candour without delay and report to the Information Commissioner's Office (ICO) within 72 hours.

Under our contracts with partners, organisations or individuals processing your **Personal Data** on our behalf are required to notify us in the event of a breach. It is then our responsibility to report to you and to the Information Commissioners Office (ICO).

Our staff are trained in the policies and procedures relating to incidents of this kind and in supporting our responsibility to you under the Duty of Candour.

Your rights under the new laws

The GDPR provides the following rights for individuals as principles, but it is important to note that these rights are NOT absolute and can be overridden by other requirements, e.g. tax, criminal law:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure *
- The right to restrict processing
- The right to data portability *
- The right to object *
- Rights in relation to automated decision making and profiling

* These rights can be complicated in the way they are governed by the law and applied in practice. Much depends upon circumstances and whether it is possible to exercise them in practice.

You have the right to be informed or to ask us to explain and give you details of how we use your Personal Data and Special Category Data. You also have the right to view your personal record and what is recorded there and our Terms and Conditions website page gives details about the process to follow. Finally you have the right to make a complaint.

We will fully explain the possible consequences to you of exercising some of the above rights as it is very important that you understand how this may affect our ability to provide care efficiently and within our usual timescales.

Can I access my information?

Information requests

If you have a request for a specific piece of information or for one of our policies or procedures, please contact us either using the online form on our website, or by calling or writing to us using the contact details below.

Under Data Protection Law , you may request access to information (with some exemptions) that is held about you and, as soon as we have verified your identity, and so long as it will not adversely affect the rights and freedoms of others, we will provide it free of charge and respond to your request within one month* of receiving it. A 'reasonable fee' can be charged for multiple copies. For 'manifestly unfounded or excessive' requests, you may be charged a fee or we may refuse to respond. Your rights to complain would not be affected.

* The period may be extended by 2 months if the request is complex or there are a number of requests. We will still respond by the initial one month period deadline, explaining that we need to extend.

For more information on how to access the information we hold about you please ask for a copy of our Subject Access Request Policy and Procedure.

You can help, use your NHS number

Every person registered with the NHS in England and Wales has their own unique NHS number. It is made up of 10 digits for example 123 456 7890. Your NHS Number is used by healthcare staff and service providers to identify you correctly. It is an important step towards improving the safety of your healthcare and helps to improve anonymous processing of patients' records.

If you do not know your NHS number, contact your GP. You may be asked for proof of identity, for example a passport or other form of identity. This is to protect your privacy. Once you have obtained your NHS Number, write it down and keep it safe. NHS Choices website has further information.

Contacting us about your information

We have a senior member of our management team who is responsible for protecting the confidentiality of your information, enabling appropriate sharing and reporting independently to our Board. Our Chief Information Officer is Bristol Community Health CIC's Data Protection Officer as defined in the Section 4 (37)(38)(39) of the GDPR.

If you have any questions or concerns regarding the information we hold on you, the use of your information or would like to discuss further, you can contact the DPO's office using any of the routes below and please let us know how you prefer us to communicate with you.

Bristol Community Health Website: 'Contact us' section, noting your query type as 'access to medical records' from the drop down list within the form.

Post: Data Protection Officer
Bristol Community Health CIC
6th Floor, South Plaza
Marlborough Street
Bristol BS1 3NX

Email: briscomhealth.dpo@nhs.net

Phone: 0117 440 9140

Contacting us if you have a complaint or concern

We strive to offer the best possible treatment and care. We try to meet the highest standards when collecting and using personal information. We welcome comments and suggestions for improving our services. We encourage people to bring concerns to our attention and we take any complaints we receive very seriously.

Complaints

If you are unhappy with how we are managing your information, please read our complaints page or download our How are we doing? leaflet.

You can submit a complaint through the Bristol Community Health Complaints Procedure, which is available on our website, or you can write to:

Patient Services Manager
Bristol Community Health CIC
6th Floor, South Plaza
Marlborough Street
Bristol BS1 3NX

Alternatively, please use the contact form on the website to send us a message, noting your query type as 'complaint' from the drop down list within the form.

If you remain dissatisfied with the BCH's decision following your complaint, you may wish to contact The Information Commissioner at the ICO. The ICO will not normally consider an appeal until you have exhausted your rights of redress and complaint to us directly. The address is:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
Website: www.ico.gov.uk

Transparency

Data Protection Law states that we must be able to explain all of the above and provide you with information on the above in clear and plain language.

If there is anything about this Privacy Notice that you do not understand or you need further information, please contact the Data Protection Officer's office on:

Tel: 0117 440 9140 or email briscomhealth.dpo@nhs.net.

What laws, rules and standards are we governed by?

The key pieces of legislation/guidance that we are governed by are:

General Data Protection Regulations (GDPR) – post 25 May 2018
Data Protection Act 1998
Human Rights Act 1998 (Article 8)
Health and Social Care Act and Regulations 2008, 2012, 2014, 2015
Equality Act 2010
Children Act 2004
Freedom of Information Act 2000
Computer Misuse Act 1990
Access to Health Records Act 1990
Copyright Design and Patents Act 1988
The Re-Use of Public Sector Information Regulations 2015
The Environmental Information Regulations 2004
Public Records Act 1958
The Common Law Duty of Confidentiality
The Care Record Guarantee for England
The Social Care Record Guarantee for England
Information Security Management Standards (ISMS)
Accessible Information Standards (AIS)
Information Security Management – NHS Code of Practice
Records Management – Code of Practice for Health and Social Care 2016

Who are we governed by?

Social Enterprise UK
Care Quality Commission
Information Commissioner's Office
Department of Health
NHS England

Our consultants, doctors, nurses, healthcare professionals and registered support staff are also regulated and governed by professional bodies including numerous royal colleges.

WEBSITE SUMMARY PRIVACY NOTICE

How do we use information about you?

Bristol Community Health CIC is committed to protecting the privacy and security of your personal information. We will only use your personal information when the law allows us to.

We collect information and then process it as part of your patient record. We use it to ensure your care is provided safely, appropriately and coordinated internally; to improve and develop our services; to investigate and learn from incidents and to correspond with you about your appointments, the care you receive and to answer any questions you may have.

It may be shared in order to make referrals to other health and social care professionals and organisations, or in emergency situations, when we are involved in audits and research, or developing joint services and if required to do so by relevant authorities, the courts or police.

We do not collect or keep information about you that we do not need and it will not be shared for marketing or other purposes.

Enquiries about the way we use your information should be directed to our Data Protection Officer.

To find out about how we collect and process information held about children using our services, please click here.

Please click here for all further information