

NHS Bedfordshire, Luton and Milton Keynes ICB Privacy Notice

What is a Privacy Notice

This Privacy Notice (sometimes known as fair processing notice) tells you about the information we collect and hold about you, what we do with it, how we will look after it and who we might share it with.

It covers information we collect directly from you or receive from other individuals or organisations.

This notice is not exhaustive. However, we are happy to provide any additional information or explanation needed. Any requests for this should be sent to:-

NHS Bedfordshire, Luton and Milton Keynes ICB
Priory House
Monks Walk
Chicksands
SHEFFORD
SG17 5TQ

Email: blmkicb.ig@nhs.net

Reviews of and Changes to our Privacy Notice

We will keep our privacy notice under regular review. This privacy notice was last reviewed in August 2025

Who we are and what we do

NHS Bedfordshire, Luton and Milton Keynes ICB is responsible for securing, planning, designing and paying for your NHS services, including planned and emergency hospital care, mental health services, rehabilitation and community services. This is known as commissioning.

This Privacy Notice is part of our programme to make transparent the data processing activities we are carrying out in order to deliver on our commissioning activities.

We also have a responsibility for arranging unplanned care services, commissioning specialist services for individual patients and supporting the system to manage a national emergency. We also monitor the performance of services to ensure they are safe, provide high quality care, meeting the needs of the local population. Part of this performance management responsibility includes responding to any concerns from patients about services.

Our Commitment to Data Protection and Confidentiality

We are committed to protecting your privacy and will only process personal confidential data in accordance with the UKGDPR and the Data Protection Act, the common law duty of confidentiality and the Human Rights Act 1998.

NHS Bedfordshire, Luton and Milton Keynes ICB is a data controller and therefore legally responsible for ensuring that all personal information is only processed in accordance data

protection legislation, and that you have the ability to exercise your rights in respect of your information.

All data controllers must register their processing activities with the Information Commissioner's Office (ICO). Our ICO Data Protection Register number is **ZB464275** and our entry can be found in the Data Protection Register on the **Information Commissioner's Office website**

Everyone working for the NHS has a legal duty to keep information about you confidential. The NHS Care Record Guarantee and NHS Constitution provide a commitment that all NHS organisations and those providing care on behalf of the NHS will use records about you in ways that respect your rights and promote your health and wellbeing.

If you are receiving services from the NHS, 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 we have a fair and lawful basis such as:

- You have given us permission;
- 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.

All information that we hold about you will be held securely and confidentially. We use administrative and technical controls to do this. We use strict controls to ensure that only authorised staff are able to see information that identifies you. Only a limited number of authorised staff have access to information that identifies you where it is appropriate to their role and is strictly on a need-to-know basis.

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

The ICB has several key roles which support the protection of your data:

- **Caldicott Guardian** - The ICB's Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing. The Guardian actively supports work to enable information sharing where it is appropriate to share and advises on options for lawful and ethical processing of information.
- **Senior Information Risk Owner (SIRO)** – The ICB's SIRO is an Executive Director with overall responsibility for an organisation's information risk policy. The SIRO is accountable and responsible for information risk across the organisation. The SIRO ensures that everyone is aware of their personal responsibility to exercise good judgement, and to safeguard and share information appropriately.

- **Data Protection Officer (DPO)** – The DPO is responsible for making sure that all information held by the ICB is collected, stored and used in accordance with the Data Protection Act 2018 and UK GDPR. The DPO is also responsible for the management and investigation of information breaches and incidents and for ensuring that the rights of individuals.

What information do we collect?

We only collect and use your information for the lawful purposes of administering the business of NHS Bedfordshire, Luton and Milton Keynes ICB.

We process personal information to enable us to support the provision of healthcare services to patients, maintain our own accounts and records, promote our services, and to support and manage our employees. To enable us to do this effectively we are often required to process personal data i.e. that which identifies a living individual.

We also process special category data. This is personal data which the Data Protection Act 2018 (DPA18) says is more sensitive, and so needs more protection:

- Racial and ethnic origin
- Offences (including alleged offences), criminal proceedings, outcomes and sentences
- Trade union membership
- Religious or similar beliefs
- Employment tribunal applications, complaints, accidents, and incident details.

This information will generally relate to our staff.

In terms of patient information, the special category data we may process:

- Physical or mental health details
- Racial and ethnic origin
- Sexual orientation
- Details of care

We will only use the minimum amount of information necessary about you.

Our records may include relevant information that you have told us, or information provided on your behalf by relatives or those who care for you and know you well, or from health professionals and other staff directly involved in your care and treatment.

Our records maybe held on paper or in a computer system. The types of information that we may collect and use include the following:

- **Personal Confidential Data:** This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this notice 'personal' includes the DPA definition of personal data, but it is adapted to include dead as well as living people. 'Confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act. Used interchangeably with 'confidential' in this document.
- **Pseudonymised Information:** This is data that has undergone a technical process that replaces your identifiable information such as a NHS number, postcode, date of birth with

a unique identifier, which obscures the ‘real world’ identity of the individual patient to those working with the data.

- **Anonymised Information:** This is data rendered into a form which does not identify individuals and where there is little or no risk of identification (identification is not likely to take place).

Information in the ICB is held for a specific length of time depending on the type of information it is. The length of time we retain your information for is defined by the NHS retention schedule which can be viewed online here: [Records Management Code of Practice for Health and Social Care 2021](#)

Once information has been reviewed and is no longer required to be kept by a retention period the information will be securely destroyed. Information is securely destroyed via an approved confidential paper and shredding recycling contractor.

Legal basis

We only use your information for lawful purposes in order for us to administer the business of the ICB effectively, and the lawful basis for the ICB to process under the Data Protection Act 2018 are:

- **Article 6 (1)(e)** Public task: the processing is necessary for the ICB to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.
- **Article 9 (2)(b)** processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union of member State law or a collective agreement pursuant to Member state law providing for appropriate safeguards for the fundamental rights and interests of the data subject.
- **Article 9 (2)(h)** processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and by means of your consent where applicable.

No automated decision-making, including profiling takes place.

How does the ICB use your information?

Although this is not an exhaustive detailed listing, the following table lists key examples of the purposes and rationale for why we collect and process information:

Purpose/Activity	Rationale
Complaints	To process your personal information if it relates to a complaint where you have asked for our help or involvement. Legal Basis We will need to rely on your explicit consent to undertake such activities.

	<p>Complaint Processing Activities</p> <p>When we receive a complaint from a person we make up a file containing the details of the complaint. This normally contains the identity of the complainant and any other individuals involved in the complaint.</p> <p>We will only use the personal information we collect to process the complaint and to check on the level of service we provide.</p> <p>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.</p> <p>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.</p> <p>We will keep personal information contained in complaint files in line with NHS retention policy. It will be retained in a secure environment and access to it will be restricted according to the ‘need to know’ principle.</p> <p>We will publish service user stories, following upheld complaints, anonymously via our governing body. The service user stories will provide a summary of the concern, service improvements identified and how well the complaints procedure has been applied. Consent will always be sought from the service user and carer or both before we publish the service user story.</p>
<p>Funding treatments</p>	<p>We will collect and process your personal information where we are required to fund specific treatment for you for a particular condition that is not already covered in our contracts.</p> <p>This may be called an “Individual Funding Request” (IFR).</p> <p>Legal Basis The clinical professional who first identifies that you may need the treatment will explain to you the information that we need to collect and process in order for us to assess your needs and commission your care and gain your explicit consent.</p>
<p>Continuing Healthcare</p>	<p>We will collect and process your identifiable information where you have asked us to undertake assessments for Continuing Healthcare (a package of care for those with complex medical needs) and commission resulting care packages.</p> <p>Legal Basis The clinical professional who first sees you to discuss your needs will explain to you the information that they need to collect and process in order for us to assess your needs and commission your care and gain your explicit consent.</p>
<p>Safeguarding</p>	<p>We will collect and process identifiable information where we need to assess and evaluate any safeguarding concerns.</p>

	<p>Legal Basis</p> <p>Because of public Interest issues, e.g. to protect the safety and welfare of vulnerable children and adults, we will rely on a statutory basis rather than consent to process information for this use.</p>
<p>Risk stratification</p>	<p>Risk stratification is a tool for identifying and predicting which patients are high risk (of health deterioration and using multiple services) or are likely to be at high risk. Prioritising the management of their care to reduce and prevent poor outcomes.</p> <p>To conduct risk stratification, national datasets are linked with GP data via your NHS Number and an algorithm is applied to produce risk scores. Risk Stratification provides focus for future demands by enabling Commissioners to prepare plans for both individual and groups of vulnerable patients who may require high levels of care. Risk Stratification also enables General Practitioners (GPs) to better target intervention to its patients.</p> <p>Legal Basis</p> <p>We are committed to conducting risk stratification effectively, in ways that are consistent with the laws that protect your confidentiality.</p> <p>The use of identifiable data for risk stratification has been approved by the Secretary of State, through the Confidentiality Advisory Group of the Health Research Authority (known as Section 251 approval). Further information on Section 251 can be obtained by clicking here.</p> <p>The reference number for the risk stratification approval is 23/CAG/0124.</p> <p>Commissioning Benefits</p> <p>Typically this is because patients have a long term condition such as Chronic Obstructive Pulmonary Disease. NHS England encourages ICBs 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.</p> <p>Knowledge of the risk profile of our population will help the ICB to commission appropriate preventative services and to promote quality improvement in collaboration with our GP practices.</p> <p>Data Processing activities for Risk Stratification</p> <p>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.</p> <p>The ICB will use pseudonymised information to understand the local population needs, whereas GPs will be able to identify which of their patients are at risk in order to offer a preventative service to them.</p>

	<p>Prescribing Services Ltd is the nominated data processor and they provide the Risk Stratification Tool which is called Eclipse.</p> <p>This processing for risk stratification is as follows:</p> <ul style="list-style-type: none"> • Identifiable SUS+ data is obtained from the SUS Repository to the Data Services for Commissioners Regional Office (DSCRO). • Data quality management and standardisation of data is completed by the DSCRO and the data identifiable at the level of NHS number is transferred securely to Prescribing Services Ltd who hold SUS+ data within a secure Data Centre . • Identifiable GP Data is securely sent from the GP system to Prescribing Services Ltd. • SUS+ data is linked to GP data in the risk stratification tool by the data processor. • As part of the risk stratification processing activity, GPs have access to the risk stratification tool within the data processor, which highlights patients with whom the GP has a legitimate relationship and have been classed as at risk. The only identifier available to GPs is the NHS numbers of their own patients. Any further identification of the patients will be completed by the GP on their own systems. • Once Prescribing Services Ltd has completed the processing, the ICB can access the online system via a secure connection to access the data Pseudonymised at patient level. <p>The risk scores are only made available to authorised users within the GP Practice where you are registered via a secure portal.</p> <p>This portal allows only the GPs to view the risk scores for the individual patients registered in their practice in identifiable form.</p> <p>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.</p> <p>Further information about risk stratification is available from: https://www.england.nhs.uk/ourwork/tsd/ig/risk-stratification/</p>
<p>Invoice Validation</p>	<p>NHS Bedfordshire, Luton and Milton Keynes is responsible for paying for health services within Bedfordshire. We are required to check healthcare invoices to ensure that they are accurate and genuine.</p> <p>To do this the ICB needs to be able to identify you so that the patient and the care provided match. Once your personal details have been used to check the validity of your care invoice, your personal details are deleted from our system before the invoice is processed for payment.</p>

	<p>Processing Activities</p> <p>The Invoice validation process involves using your NHS number and occasionally your postcode or date of birth to establish which NHS organisation is responsible for paying for your treatment. The information is only accessible by named staff in a controlled environment.</p> <p>This activity is undertaken in house for Bedfordshire, Luton and Milton Keynes patients.</p> <p>Legal Basis</p> <p>The Secretary of State for Health has approved the NHS England application for support under Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002 (Section 251 Support). This allows Clinical Commissioning Groups (ICBs) and Commissioning Support Units (CSUs) to process Personal Confidential Data (PCD) which are required for invoice validation purposes. .</p>
<p>Patient and Public Involvement</p>	<p>If you have asked us to keep you regularly informed and up to date about the work of the ICB 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 share with us.</p> <p>Legal Basis We will rely on your consent for this purpose</p> <p>Benefits Where you submit your details to us for involvement purposes, we will only use your information for this purpose. You can opt out at any time by contacting us using our contact details at the end of this document.</p>
<p>Commissioning</p>	<p>To collect NHS data about service users that we are responsible for.</p> <p>Legal Basis</p> <p>Our legal basis for collecting and processing information for this purpose is statutory.</p> <p>Processing Activities</p> <p>Hospitals and community organisations that provide NHS-funded care must submit certain information to NHS Digital about services provided to our service users.</p> <p>This information is generally known as commissioning datasets. The ICB obtains these datasets from NHS Digital and they relate to service users registered with GP Practices that are members of the ICB.</p> <p>These datasets are then used in a format that does not directly identify you, for wider NHS purposes such as managing and funding the NHS, monitoring activity to understand and plan the health needs of the population and to gain evidence that will improve health and care through research.</p>

	<p>The datasets include information about the service users who have received care and treatment from those services that we are responsible for funding. The ICB is unable to identify you from these datasets. They do not include your name, home address, NHS number, post code or date of birth. Information such as your age, ethnicity and gender as well as coded information about any clinic or accident and emergency attendances, hospital admissions and treatment will be included.</p> <p>The specific terms and conditions and security controls that we are obliged to follow when using those commissioning datasets can also be found on https://digital.nhs.uk/services/secondary-uses-service-sus.</p> <p>We also receive similar information from GP Practices within our ICB membership that does not identify you. We use this datasets for a number of purposes such as:</p> <ul style="list-style-type: none"> • Performance managing contracts; • Reviewing the care delivered by providers to ensure service users are receiving quality and cost effective care; • To prepare statistics on NHS performance to understand health needs and support service re-design, modernisation and improvement; • To help us plan future services to ensure they continue to meet our local population needs; • To reconcile claims for payments for services received in your GP Practice; • To audit NHS accounts and services; <p>If you do not wish your information to be included in these datasets, even though it does not directly identify you, Email: enquiries@nhsdigital.nhs.uk (please include “national data opt-out policy”) within the subject line. Telephone: (contact centre): 0300 303 5678.</p>
<p>For Other organisations to provide support services for us</p>	<p>This often involves those organisations processing data on our behalf.</p> <p>Legal Basis</p> <p>Statutory requirement for NHS Digital to collect identifiable information. A Section 251 approval from the Secretary of State, through the Confidentiality Advisory Group of the Health Research Authority, enables the use of pseudonymised information about patients included in the datasets, by the organisations who submitted the information.</p> <p>There is no requirement for a legal basis for use of the aggregated information which is available to the ICB as this does not identify individuals.</p> <p>DATA PROCESSORS</p>

	<p>Below are details of our data processors and the function that they carry out on our behalf:</p> <ul style="list-style-type: none"> • Circle MSK - Provide a musculo skeletal triaging service for the ICB • Oasis – Archiving of records. • RSR Consultants – Provide a service for detecting, counting and coding changes. • Prescribing Services Ltd – Will be providing a Risk Stratification service for the ICB. • NHS Arden & GEM CSU – process secondary uses of data for Bedfordshire, Luton and Milton Keynes ICB <p>These organisations are subject to the same legal rules and conditions for keeping personal confidential data secure and are underpinned by a contract with us. Before awarding any contract, we ensure that organisations will look after your information to the same high standards that we do. Those organisations can only use your information for the service we have contracted them for and cannot use it for any other purpose. Other NHS organisations can act as Data Processors with the same legal rules and conditions applying and with contracts and agreements required to be in place.</p> <p>Benefits</p> <p>These organisations are subject to the same legal rules and conditions for keeping personal confidential data and secure and are underpinned by a contract with us.</p> <p>Before awarding any contract, we ensure that organisations will look after your information to the same high standards that we do. Those organisations can only use your information for the service we have contracted them for and cannot use it for any other purposes.</p>
<p>National Registries</p>	<p>National Registries (such as the Learning Disabilities Register) have statutory permission under Section 251 of the NHS Act 2006, to collect and hold service user identifiable information without the need to seek informed consent from each individual service user.</p>
<p>Research</p>	<p>To support research oriented proposals and activities in our commissioning system</p> <p>Legal Basis</p> <p>Your consent will be obtained by the organisation holding your records before identifiable information about you is disclosed for any research.</p> <p>Sometimes research can be undertaken using information that does not identify you. The law does not require us to seek your consent in this case, but the organisation holding your information will make notices available on the premises and on the website about any research projects that are undertaken.</p>

	<p>Benefits</p> <p>Researchers can provide direct benefit to individuals who take part in medical trials and indirect benefit to the population as a whole.</p> <p>Service user records can also be used to identify people to invite them to take part in clinical trials, other interventional studies or studies purely using information from medical records.</p> <p>Processing Activities</p> <p>Where identifiable data is needed for research, service users will be approached by the organisation where treatment was received, to see if they wish to participate in research studies.</p>
<p>Fraud Prevention</p>	<p>NHS Bedfordshire, Luton and Milton Keynes ICB is required by law to protect the public funds it administers. It may share information provided to it with other bodies responsible for auditing or administering public funds, in order to prevent and detect fraud.</p> <p>The Cabinet Office conducts data matching exercises to assist in the prevention and detection of fraud. This is one of the ways in which the Minister for the Cabinet Office takes responsibility within government for public sector efficiency and reform. The Minister for the Cabinet Office is also the Chair of the Fraud, Error and Debt Taskforce, the strategic decision-making body for all fraud and error, debt and grant efficiency initiatives across government.</p> <p>Data matching involves comparing sets of data, such as the payroll or benefits records of a body, against other records held by the same or another body to see how far they match. The data is usually personal information. The data matching allows potentially fraudulent claims and payments to be identified. Where a match is found it may indicate that there is an inconsistency that requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.</p> <p>The processing of data by the Cabinet Office in a data matching exercise is carried out with statutory authority under its powers in Part 6 of the Local Audit and Accountability Act 2014. It does not require the consent of the individuals concerned under the Data Protection Act 2018.</p> <p>All bodies participating in the Cabinet Office's data matching exercises receive a report of matches that they should investigate, so as to detect instances of fraud, over- or under-payments and other errors, to take remedial action and update their records accordingly.</p>

Your Rights

The UK GDPR gives you (or your authorised representative e.g. somebody who has Power of Attorney to deal with your affairs) the right to request the following:

- **The right to be informed**

You have the right to be informed about the collection and use of your personal data. This privacy notice is one of BLMK ICB's key methods for providing you with this information. In addition to this notice, we will provide you with more specific information at the time we collect personal data from you, such as when you apply for Continuing Healthcare or make a complaint to us.

- **The right of access**

UK GDPR gives you (or your authorised representative e.g. somebody who has Power of Attorney to deal with your affairs) the right to ask us for confirmation of whether we process data about you and if we do, to have access to that data so you are aware and can verify the lawfulness of the processing.

This is known as 'the right of access', also more commonly known as a Subject Access Request (SAR).

Some individuals may also have the right (under the Access to Health Records (Deceased) Act), to request and be provided with information we hold about a deceased individual. However, strict exemptions do apply.

You can make your own application to see the information we hold about you, or you can authorise someone else to make an application on your behalf. A child's parent or guardian, a patient representative, or a person appointed by the court may also apply.

- **The right to rectification**

You are entitled to have personal data that we hold about you rectified if it is inaccurate or incomplete. If we have passed the data concerned on to others, we will contact each recipient and inform them of the rectification – unless this proves impossible or involves disproportionate effort. If this is the case, we will explain to you why.

- **The right to erasure**

You have the right to have personal data we hold about you erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- If you withdraw your consent for us to process your data (if this was the basis on which it was collected).
- The personal data was unlawfully processed (i.e. a breach of UK data protection laws).
- The personal data has to be erased in order to comply with a legal obligation.

However, if we have collected and are processing data about you to comply with a legal obligation for the performance of a public interest task or exercise of official authority, i.e. because we have a legal duty to do so in our functioning as a ICB, then the right to erasure does not apply.

- **The right to restrict processing**

You have the right to ‘block’ or suppress processing of your personal data which means that if you exercise this right, we can still store your data but not to further process it and will retain just enough information about you to ensure that the restriction is respected in future.

You can ask us to restrict the processing of your personal data in the following circumstances:

- If you contest the accuracy of the data, we hold about you we will restrict the processing until the accuracy of the data has been verified.
- If we are processing your data as it is necessary for the performance of a public interest task and you have objected to the processing, we will restrict processing while we consider whether our legitimate grounds for processing are overriding.;
- If the processing of your personal data is found to be unlawful but you oppose erasure and request restriction instead; or
- If we no longer need the data we hold about you, but you require the data to establish, exercise or defend a legal claim.

If we have disclosed the personal data in question to others, we will contact each recipient and inform them of the restriction on the processing of the personal data – unless this proves impossible or involves disproportionate effort. If asked to, we must also inform you about these recipients.

We will inform you if we decide to lift a restriction on processing.

- **The right to data portability**

The right to data portability allows you to obtain and reuse your personal data for your own purposes across different services. It allows you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability although it only applies where we are processing your personal data based on your consent for us to do so or for the performance of a contract and where the processing is carried out by automated means. This means that currently, the ICB does not hold any data which would be subject to the right to data portability.

- **The right to object**

Where the ICB processes personal data about you based on being required to do so for the performance of a task in the public interest/exercise of official authority, you have a right to object to the processing.

You must have an objection on grounds relating to your particular situation.

If you raise an objection, we will no longer process the personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or the processing is for the establishment, exercise or defence of legal claims.

- **Rights in relation to automated decision making and profiling**

As the ICB does not make any decisions based solely on automated processing, individuals' rights in relation to personal data processed in this way are not applicable.

- **The right to withdraw consent**

If the ICB processes data about you on the basis that you have given your consent for us to do so, you have the right to withdraw that consent at any time. Where possible, we will make sure that you are able to withdraw your consent using the same method as when you gave it.

If you withdraw your consent, we will stop the processing as soon as possible.

The NHS Constitution states, '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'. There may be occasions when it is not possible to exercise your right to object or 'Opt Out', such as when we have an obligation by law or for the purposes of safeguarding adults and children.

The right to object or opt-out includes information not directly collected by the ICB, but collected by organisations that provide NHS services.

How do I apply my rights?

If you like to apply for any of your rights detailed above, please contact the IG team via blmkicb.ig@nhs.net.

If you wish to ask us for confirmation of whether we process data about you or access your personal data, then please complete the following form [Subject Access & Access to Health Records Request form](#) or and contact: blmkicb.ig@nhs.net

If you are unable to print the form, please email our IG Department who will be happy to assist you blmkicb.ig@nhs.net.

To submit a request please complete the form and send it to us as instructed in the form. Following receipt of your form we will do all we can to provide you with the requested information within 30 calendar days.

Please note that when applying for you rights we will ask to verify your identification.

Exercising an Opt-out

- **Information directly collected by the ICB**

Your right can be exercised by withdrawing your consent for the ICB to share information you have provided directly to us that identifies you, provided there is no overriding legal obligation

for us to share your personal information. Where we cannot comply with your request, we will provide you with full details of the reason why. You can withdraw your consent in writing to the ICB, using the contact details within this Notice.

- **Information collected by the ICB from organisations that provide NHS services**

Whenever you use a health or care service, such as attending Accident & Emergency or using Community Care services, important information about you is collected in a patient record for that service. Collecting this information helps to ensure you get the best possible care and treatment.

The information collected about you when you use these services can also be used and provided to other organisations for purposes beyond your individual care, for instance to help with:

- Improving the quality and standards of care provided
- Research into the development of new treatments
- Preventing illness and diseases
- Monitoring safety
- Planning services.

This may only take place when there is a clear legal basis to use this information. All these uses help to provide better health and care for you, your family and future generations. Confidential patient information about your health and care is only used like this where allowed by law.

Most of the time, anonymised data is used for research and planning so that you cannot be identified in which case your confidential patient information isn't needed.

You have a choice about whether you want your confidential patient information to be used in this way. If you are happy with this use of information you do not need to do anything. If you do choose to opt-out your confidential patient information will still be used to support your individual care.

Your choice to opt-out will have no negative impact on your individual care.

By setting your opt-out preferences at a national level, NHS Digital and Public Health England will exclude your confidential information (i.e. information that identifies you and your health data) from any anonymised information shared with commissioners and research bodies.

NHS Bedfordshire, Luton and Milton Keynes ICB meets the requirements of the National Data Opt Out.

You can check or update your opt-out preference via the following link:

<https://www.nhs.uk/your-nhs-data-matters/manage-your-choice/>

- **Type 1 opt-out**

If you do not want personal confidential data that identifies you to be shared outside your GP practice, for purposes beyond your individual care, you can register a 'Type 1 opt-out' with your GP practice. This prevents your personal confidential information from being used for anything

except your care, except when it is required by law, such as a public health emergency like an outbreak of a pandemic disease.

Patients are only able to register this opt-out at their GP practice. If you would like to opt-out or discuss further, then please talk to your GP or the healthcare professional supporting you.

Complaints or questions

We try to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring concerns to our attention if they think that our collection or use of information is unfair, misleading or inappropriate. We would also welcome any suggestions for improving our procedures.

If you have any questions or concerns regarding how we use your information, please contact us at:

NHS Bedfordshire, Luton and Milton Keynes ICB

Priory House,
Monks Walk,
Chicksands
SHEFFORD
SG17 5TQ

blmkicb.ig@nhs.net

For independent advice about data protection, privacy and data-sharing issues, you can contact the:

Information Commissioner
Wycliffe House, Water Lane,
Wilmslow,
Cheshire, SK9 5AF.
Phone: 08456 30 60 60 or 01625 54 57 45
Website: www.ico.gov.uk

The Data Protection Officer for the ICB is:

Roz Samuel
Head of Safe Practice and Data Protection Officer
Email: blmkicb.ig@nhs.net