NHS Frimley Integrated Care Board

Your Personal Information – what you need to know

Who we are and what we do

NHS Frimley Integrated Care Board (ICB) is responsible for securing, planning, designing and paying for your NHS services, including planned and emergency hospital care, as well as community and primary medical care (GP) services. We also have a performance monitoring role for these services, which includes ensuring that the highest quality of healthcare is provided and responding to any concerns from our patients on services offered. This is known as commissioning. For further information please refer to the ICB website.

Our Commitment to Data Privacy and Confidentiality Issues

We are committed to protecting your privacy and will only process data in accordance with the Data Protection Legislation. This includes the General Data Protection Regulation (EU) 2016/679 (GDPR), the Data Protection Act (DPA) 2018, the Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws implementing them as amended from time to time.

In addition, consideration will also be given to all applicable Law concerning privacy, confidentiality, the processing and sharing of personal data including the Human Rights Act 1998, the Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations.

The ICB is a Data Controller as defined under the GDPR. We are legally responsible for ensuring that all personal information that we process i.e., hold, obtain, record, use or share about you, is done in compliance with the six Data Protection Principles as set out in Article 5 under GDPR.

All data controllers must notify the Information Commissioner's Office (ICO) of all personal information processing activities. Our ICO Data Protection Registration number is ZA845096, 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.

The 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, or where undertaking a public function, to prevent and detect fraud.

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 a limited

number of authorised staff can 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 role 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.

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

We will only retain information in accordance with the schedules set out in the Records Management Code of Practice.

What kind of information do we use?
As a commissioner we do not routinely hold or have access to your medical records. However, we may need to hold some personal information about you, for example:

- Your name, address, your date of birth, contact details and your NHS number which in some circumstances we may use as your single identifying number with no other information about you attached. Your NHS number is present in all your health records and therefore we can use that number to link information to you or about you without revealing any personal or confidential data, where we are lawfully allowed to do this.
- Details of your GP, what treatment you have received and where you received it
- Details of concerns or complaints you have raised about your healthcare provision, and we need to investigate
- Details of clinical concerns raised by your General Practitioner (GP) or service providers about your healthcare provision
- If you ask us for our help or involvement with your healthcare, or where we are required to fund specific specialised treatment for a particular condition that is not already covered in our contracts with organisations that provide NHS care
- If you ask 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 service user/Patient Participation Groups

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 may be held on paper or in a computer system.

We use the following types of information/data:

- **Personal Data** – means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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 natural person. Article 4 of the GDPR
- **Special Categories of Personal Data** – this term describes 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. Article 9 of the GDPR
- **Confidential Patient Information** – this term describes information or data relating to their health and other matters disclosed to another (e.g., patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. Including both information 'given in confidence' and 'that which is owed a duty of confidence'. As described in the Confidentiality: NHS code of Practice: Department of Health guidance on confidentiality 2003.
- **Pseudonymised** – this is data that has undergone a technical process that replaces your identifiable information such as 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** – this is data about individuals but with identifying details removed so that there is little, or no risk of the individual being re-identified
- **Aggregated** – anonymised information that is grouped together so that it does not identify individuals

What do we use your personal and special categories of personal data for?

There are some limited exceptions where we may hold and use personal data and special categories of personal data about you. For example, the ICB is required by law to perform certain services that involve the processing of these data types.

The areas where we use personal data and special categories of personal data include:

- responding to your queries, compliments or concerns
- assessment and evaluation of safeguarding concerns

We may also use this data in the following cases:

- the information is necessary for your direct healthcare needs
- we need to respond to patients, carers or Member of Parliament communications
- you have freely given your explicit agreement (consent) for us to use your information for a specific purpose
- there is an overriding public interest in using the information e.g., to safeguard an individual, or to prevent a serious crime

- there is a legal requirement that will allow us to use or provide information (e.g., a formal court order).

For what do we use non-identifiable data?
We use pseudonymised, anonymised and aggregated data to plan health care services. Specifically, we use it to:

- check the quality and efficiency of the health services we commission
- prepare performance reports on the services we commission
- work out what illnesses people may have in the future, so we can plan and prioritise services and ensure these meet the needs of patients in the future
- review the care being provided to make sure it is of the highest standard
- evaluate the services we have or have been commissioned on our behalf
- support the regional and national initiatives through the Integrated Care Systems (ICS) or the Sustainability and Transformation Plan (STP)

Do we share your information with other organisations?
We commission a number of organisations (both within and outside the NHS) to provide healthcare services to you. We may also share anonymised and aggregated statistical information with them for the purpose of improving local services, research, audit and public health; for example, understanding how health conditions spread across our local area compared against other areas.

We work in collaboration with other Commissioners to jointly commission services. These require the inter-sharing of statistical information for the purposes of improving those services commissioned and the health outcomes of our population.

We would not share information that identifies you unless we have a fair and lawful basis such as:

- you have given us explicit consent
- we need to act to protect children and vulnerable adults
- when a formal court order has been served upon us
- 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 there is an overriding public health interest e.g., communicable diseases as instructed by NHS England
- when permission is given by the Secretary of State or the Health Research Authority on the advice of the Confidentiality Advisory Group to process personal and special categories of personal data without the explicit consent of individuals

The Health and Social Care Act 2012 provides some NHS bodies, particularly NHS Digital (formally the Health and Social Care information Centre) ways of collecting and using patient data that cannot identify a person to help Commissioners to design and procure the combination of services that best suit the population they serve.

How we process information within the ICB

The ICB contracts with other organisations to process data on our behalf. These organisations are known as 'Processors' and we ensure they are legally and contractually bound, providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the General Data Protection Regulation (GDPR) and ensure the protection of the rights of the data subject.

Data may be anonymised and linked with other data so that it can be used to improve healthcare and development and monitor NHS performance. Where data is used for these statistical purposes, stringent and technical measures are taken to ensure individual patients cannot be identified.

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 data from your Doctor (GP) with other data such as hospital inpatient stays, outpatient appointments and A&E attendances; this type of data is called secondary uses service (SUS) data. In some cases, there may also be a need to link local datasets which could include a range of other hospital-based services such as radiology, physiotherapy, audiology etc., as well as mental health and community-based clinics and services such as district nursing, podiatry etc. When conducting this analysis, the linkage of these datasets is always done using a pseudonym (unique identifier), applied by NHS Digital, which does not reveal a person's identity, as the ICB does not have any access to identifiable data for these purposes.

A full list of details including the legal basis, any Data Processor involvement and the purposes for processing information can be found in Appendix A.

What safeguards are in place to ensure data that identifies you is secure?

We only use information that may identify you in accordance with the data protection legislation (as defined in the Data Protection Act 2018). The data protection legislation requires us to process personal data only if there is a legitimate/legal basis for doing so and that any processing must be fair, lawful and transparent.

Within the health sector, we also must follow the common law duty of confidentiality, which means that where identifiable information about you has been given in confidence, it should be treated as confidential and only shared for the purpose of providing direct healthcare.

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.

The Confidentiality: NHS Code of Practice applies to all of our staff, and they are required to protect your information, inform you of how your information will be used, and allow you to decide if and how your information can be shared. All ICB staff are expected to make sure information is kept confidential and receive annual training on how to do this. This is monitored by the ICB and can be enforced through disciplinary procedures.

We also ensure the information we hold is kept in secure locations, restrict access to information to authorised personnel only, protect personal and confidential information held on equipment such as

laptops with encryption (which masks data so that unauthorised users cannot see or make sense of it).

We ensure external data processors that support us are legally and contractually bound to operate and prove security arrangements are in place where data that could or does identify a person are processed.

Accountability
The ICB has a senior member of staff responsible for protecting the confidentiality of patient information. This person is called the Caldicott Guardian. The contact details of our Caldicott Guardian are as follows:

Sarah Bellars
Chief Nursing Officer
Director of Infection, Prevention and Control (DIPC)
Email: FrimleyICB.caldicottguardian@nhs.net

The Caldicott Guardian is supported by another senior member of staff who is responsible for information risk and information security, this person is called the Senior Information Risk Owner (SIRO). The contact details of our SIRO are as follows:

Sam Burrows
Chief Transformation Officer
Email: FrimleyICB.siro@nhs.net

The Data Protection Officer (DPO) is responsible for monitoring compliance against the data protection legislations (GDPR & DPA 2018), Information Governance (IG) policies, providing advice and guidance, raising awareness, training and audits. The DPO acts as a contact point for the ICO, employees and the public. They co-operate with the ICO and will consult on any other matter relevant to Data Protection. The contact details of our DPO are as follows:

Nicola Gould
Data Protection Officer
Email: FrimleyICB.dpo@nhs.net

The ICB is registered with the Information Commissioner's Office (ICO) as a data controller and collects data for a variety of purposes. Our registration number is [Registration Number] and a copy of the registration is available through the ICO website.

How long do we hold information for?
The ICBs approach to the management of its business records are in line with national guidance from NHS Digital, Records Management Code of Practice. The code of practice sets out the best practice for NHS organisations to follow. To ensure compliance the ICB's records shall not be retained indefinitely and once information that we hold has been identified for destruction it will be disposed of in the most appropriate way for the type of information it is. Confidential information (whether personal or commercially) will be disposed of by approved and secure confidential waste procedures. We keep a record of retention schedules within our information asset registers.

Your right to opt out of data sharing and processing
The NHS Constitution states, 'You have a right to request that your personal confidential information is not used beyond your own direct care and treatment and to have your objections considered'. For further information please see the NHS Constitution.

Direct care is defined as a clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation or suffering of an individual.

Indirect care is defined as work within the health and social care environment which does not involve the direct treatment or support of individuals e.g., research, commissioning and much of the work done in public health.

There are several forms of opt- outs available at various levels. These include for example:

Information directly collected by the ICB. Your choices can be exercised by withdrawing your consent for the sharing of information that identifies you unless there is an overriding legal obligation. We will first need to explain how this may affect the care you receive but you can do this by writing to us.

Information not directly collected by the ICB but collected by organisations that provide NHS services. These are known as Type 1 and National data opt-outs (previously Type 2) and are described below:

Type 1 opt-out
If you do not want personal confidential information that identifies you to be shared outside your GP practice, for purposes beyond your direct care, you can register a 'Type 1 Opt-Out' with your GP practice. This prevents your personal confidential information from being used other than circumstances required by law, such as a public health emergency like an outbreak of a pandemic disease.

Patients are only able to register an opt-out at their GP practice.

Records for patients who have registered a 'Type 1 Opt-Out' will be identified using a particular code that will be applied to your medical records that will stop your records from being shared outside of your GP Practice.

National data opt-out
National data opt-out. The national data opt-out was introduced on 25 May 2018, enabling patients to opt-out from the use of their data for research or planning purposes, in line with the recommendations of the National Data Guardian in her Review of Data Security, Consent and Opt-Outs.

All health and care organisations are required to apply national data opt-outs where confidential patient information is used for research and planning purposes. NHS Digital has been applying national data opt-outs since 25 May 2018. Public Health England has been applying national data opt-outs since September 2018.

The national data opt-out replaces the previous 'type 2' opt-out, which required NHS Digital not to share a patient's confidential patient information for purposes beyond their individual care. Any

patient that had a type 2 opt-out recorded on or before 11 October 2018 has had it automatically converted to a national data opt-out. Those aged thirteen or over were sent a letter giving them more information and a leaflet explaining the national data opt-out. The deadline for health and care organisations to comply with national data opt-out policy is currently the end of March 2021. It has been extended to enable health and care organisations to focus their resources on the coronavirus (COVID-19) outbreak. For more information go to National data opt out programme.

The use of personal confidential data by ICBs for invoice validation under approval reference (CAG 7-07)(a-c)/2013) has been recently extended to the end of September 2022 and as part of that review, it has been agreed that no opt out will be applied to invoice validation due to the importance of accurately allocating NHS resources and the lack of evidence of public concern in relation to the use of data for this specific purpose. This effectively means that data which includes an identifier (usually NHS number) which is flowing from NHS Digital to commissioners for invoice validation/challenge purposes will be provided for all patients to ensure that providers receive the correct funding for the health and care services they provide.

To find out more visit the NHS Digital website opting out pages.

Gaining access to the data we hold about you
Exercising the Right of Access (Subject Access Requests)

Individuals can find out if we hold any personal information by making a request under the Right of Access under the GDPR, more commonly called a 'Subject Access Request'. If we do hold information about you, we will.

- Give you a description of it
- Tell you why we are holding it
- Tell you who it could be disclosed to
- Let you have a copy of the information in an intelligible form
- Correct any mistakes to information held

Everybody has the right to see, or have a copy, of data we hold that can identify you, with some exceptions. You do not need to give a reason to see your data, but you may be charged a fee.

If you want to access your data, you must make the request in writing. Under special circumstances, some information may be withheld.

For further information on how to make a request please visit our policies and procedures page on our website.

If you require further advice, please email your request to:

Email: FrimleyICB.dpo@nhs.net

What is the right to know?
The Freedom of Information Act 2000 (FOIA) gives people a general right of access to information held by or on behalf of public authorities, promoting a culture of openness and accountability across the public sector. You can request any information that the ICB holds, that does not fall under an

exemption. You may not ask for information that is covered by the Data Protection Act under FOIA. However, you can request this under a Subject Access Request – see section above 'Gaining access to the data we hold about you'.

Your request must be in writing and can be either posted or emailed to:

By Email: frimleyICB.foi@nhs.net

By Post:
Freedom of Information
NHS Frimley ICB
Aldershot Centre for Health
Hospital Hill
Aldershot
GU11 1AY

Please be advised that requests received via the postal service will not be processed until such time that staff are able to return to their offices.

For further information please visit the ICB's FOI page on our website.

Information Commissioners Office
For independent advice about data protection, privacy, data sharing issues and your rights you can contact:

By post: Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

By telephone: 0303 123 1113 (local rate) or 01625 545 745

By email: casework@ico.org.uk or visit the ICO website.

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. You can contact us by:

By telephone: 0300 561 0250 By email: scwcsu.palscomplaints@nhs.net

For further information go to our website.

Your Rights
GDPR provides the following rights for individuals:

- 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.

Overseas Transfers
Your information will not be sent outside of the UK where the laws do not protect your privacy to the same extent as the law in the UK and or in compliance with the General Data Protection Regulations. We will never sell any information about you.

Automated Decision Making
The ICB will not make decisions based solely on automated processing

Links to other websites
This Privacy Notice does not cover the links within ICB's website linking to other websites or other organisations. We encourage you to read the privacy statements on the other websites you visit.

Changes to this privacy notice
We keep our Privacy Notice under regular review. This Privacy Notice was last updated in April 2021.

Further information
Further information about the way in which the NHS uses personal confidential data and your rights in that respect can be found at:

NHS Digital: NHS Digital are the national information and technology partner to the health and social care system. NHS Digital are using digital technology to transform the NHS and social care. They also have responsibility for standardising, collecting and publishing data and information from across the health and social care system in England. You can find out more about NHS Digital here.

NHS Digital – Guide to Confidentiality: NHS Digital are also the trusted national provider of high-quality information, data and IT systems for health and social care and are responsible for collecting data from across the health and social care system.

The NHS Constitution: The Constitution establishes the principles and values of the NHS in England. It sets out rights to which patients, public and staff are entitled, and pledges which the NHS is committed to achieve, together with responsibilities, which the public, patients and staff owe to one another to ensure that the NHS operates fairly and effectively.

To share or not to share? Information Governance Review: This was an independent review of information about service users shared across the health and care system led by Dame Fiona Caldicott and was conducted in 2012.

Information Commissioner's Office (ICO): The ICO is the Regulator for GDPR and offer independent advice and guidance on the law and personal data, including your rights and how to access your personal information.

Health Research Authority: The HRA protects and promotes the interests of patients and the public in health and social care research.

Our uses of Information

Activity	Rationale
Complaints	**Purpose** – To process your personal information if it relates to a complaint where you have asked for our help or involvement. For contact details please see the ICB's contact us or visit our website. **Legal Basis** - The ICB has a duty as to the improvement in quality of services under Section 14R NHS Act 2006 and will rely on your explicit consent as the basis to undertake such activities. **Benefits** - Managing complaints enables the ICB to continuously improve the quality of the services they commission. **Retention period** - Information relating to complaints will be retained for 10 years after which time the information will be reviewed and if no longer necessary will be destroyed.
Freedom of Information (FOI) requests	**Purpose** – We may need to process your personal information where we are requested to fund specific treatment for you for a particular condition that is not already covered in our contracts. **Legal Basis** – The National Health Service Commissioning Board and Clinical Commissioning Groups (Responsibilities and Standing Rules) Regulations 2012 part 7 (34) sets out the duty of an ICB regarding funding and commissioning of drugs and other Treatments. The clinical professional who first identifies that you may need the treatment will explain to you the information that is needed to be collected and processed to assess your needs and commission your care; they will gain your explicit consent to share this. **Benefits** – leads to easier information access and greater public awareness of laws, rules, regulations, policies and procedures
Individual Funding Requests	**Purpose** – We will collect and process your personal information where we are requested to fund a specific treatment or service for a condition that is not routinely offered by the NHS. This is called an "Individual Funding Request" (IFR). **Legal Basis** –The National Health Service Commissioning Board and Clinical Commissioning Groups (Responsibilities and Standing Rules) Regulations 2012 part 7 (34) sets out the duty of an ICB regarding funding and commissioning of drugs and other Treatments. The clinical professional who first identifies that you may need the treatment will explain to you the information that is needed

	to be collected and processed to assess your needs and commission your care; they will gain your explicit consent to share this. **Benefits** - The Individual Funding Request process allows the ICB to look at evidence for the safety and effectiveness of any treatment and ensures that the services we pay for will give patients the greatest health gains from the finite resources we have available. **Retention period** - Information relating to Individual Funding Requests will be retained for 2 years if funding is rejected and 8 years if funding is accepted after which time the information will be reviewed and if no longer necessary will be destroyed.
Continuing Healthcare (CHC)	**Purpose** – We will collect and process your identifiable information where you have asked us to undertake assessments for your continuing healthcare which is a package of care that is arranged and funded solely by the NHS for individuals who are not in hospital but have been assessed as having a "primary health need". This is called "Continuing Health Care" (CHC) **Legal Basis** - The ICB has a duty to have regard to the need to reduce health inequalities in access to health services and health outcomes achieved as outlined in the National Health Service Commissioning Board and Clinical Commissioning Groups (Responsibilities and Standing Rules) Regulations 2012 (SI 2012 No 2996) (Part 6-20-22. The clinical professional who first sees you to discuss your needs will explain to you the information that they need to collect and process for us to assess your needs and commission your care and will ask for your informed consent for personal clinical information to be shared with the ICB. **Benefits** – Frimley ICB can arrange a care and support package that meets your assessed needs. The ICB can determine how your needs and care will be managed, where your care will be given e.g., in your own home or in a care home and identify which organization will be responsible for meeting your needs. **Retention Period** - Information relating to Continuing Healthcare will be retained for 8 years after which time the information will be reviewed and if no longer necessary will be destroyed.
Collaborative fees part of Mental	GPs from different geographic areas send their Mental Health Assessment Claim forms to Berkshire Healthcare Foundation Trust,

Health Assessment Claims	West Hampshire ICB and South Central and West CSU depending upon their location. The purpose of the involvement of the Finance teams with regards to Mental Health Assessment Claim work stream is to process the claim and approve payment to the assessing doctor for working during out of hours or on weekends. The information that the Finance Team will have access to includes patient's full name, address, D.O.B, NHS number, Registered GP of the patient, name of the assessing doctor, date and time of the assessment, and information on the outcome of the assessment. Legal Basis - The lawful basis which ensures that Southampton ICB are processing your information correctly is Article 6(1)b (contractual relationship) and Article 9(2)c (processing is necessary to protect the vital interests of an individual). Frimley ICB will only keep your information for as long as necessary. The information will be retained in a secure environment and access to it will be restricted according to the 'need to know' principle. As with all the information that we process about you, you have several rights that apply to your personal information. These can be found in the "Your Rights" section.
Safeguarding	**Purpose** – Safeguarding means protecting peoples' health, wellbeing and human rights, and enabling them to live free from harm, abuse and neglect. It is key in providing high-quality health and social care. The ICB, as an NHS statutory organisation has a duty to participate in Serious Case Reviews for children and adults and Domestic Homicide Reviews undertaken by either the local Children's Partnership Safeguarding Boards, the Adult Safeguarding Boards or the Community Safety Partnership for continued learning, to minimize risk and to improve services. **Legal Basis** - The ICB has a statutory responsibility under the Children Act 2004, Care Act 2014 and safeguarding provision within the Data Protection Act 2018 – Schedule 1, Part 2, subsections 18 and 19 to ensure the safety of all children, and the safety of adults at risk of abuse and neglect. This is not finite; legislation is reviewed, updated and incorporated according to safeguarding risks and responsibilities. **Benefits** - Safeguarding is a fundamental element of the ICBs commissioning plans and forms a core part of the commissioning assurance process. **Retention period** - The ICB will hold your information for a period of 8 years following the closure of a case. Before records are destroyed, we will review information held and consider any serious incident retentions which may require us to hold the information for a further period. Each case will be reviewed on an individual basis.

Invoice Processing and Validation	**Purpose** – The Invoice Validation process ensures that care providers who provide you with care and treatment can be paid for the services they provide in a timely and efficient manner. There are situations where personal data is required to ensure that the correct service provider is paid. In such cases service providers are required to send identifiable patient personal identifiable data such as NHS Number to a Controlled Environment for Finance (CEfF) which is a secure restricted area within SCWCSU who process this data on our behalf and indicate which invoices we can validate (authorize) for payment. NHS England has published guidance on how invoices must be processed and Commissioners have a duty to detect report and investigate any incidents of where a breach of confidentiality has been made. NHS SBS do not require and should not receive any personal data to provide their services. **Legal Basis** - GDPR Art. 6(1) (e) and Art.9 (2) (h). The use of personal confidential data by ICBs for invoice validation has been approved by the Secretary of State, through the Confidentiality Advisory Group of the Health Research Authority (approval reference (CAG 7-07)(a-c)/2013)) and this approval has been extended to the end of September 2022 NHS England Invoice Validation which gives us a statutory legal basis under Section 251 of the NHS Act 2006 to process data for invoice validation purposes which sets aside the duty of confidentiality. We are committed to conducting invoice validation effectively, in ways that are consistent with the laws that protect your confidentiality. Benefits – The invoice validation process supports the delivery of patient care by ensuring that: • service providers are paid for patients' treatment, • enables services to be planned, commissioned, managed and subjected to financial control, • enables commissioners to confirm that they are paying appropriately for the treatment of patients for whom they are responsible • fulfilling commissioners' duties of fiscal probity and scrutiny • enables invoices to be challenged and disputed or discrepancies resolved **Retention period** - Information relating to Invoice Validation will be retained for 3 years.

Medicines Optimisation	**Purpose** - Medicines Optimisation is about ensuring that the right patients get the right choice of medicine at the right time. By focusing on patients and their experiences, the goal is to help patients to improve their outcomes, take their medicines correctly, avoid taking unnecessary medicines, reduce wastage of medicine and improve medicines safety. Medicines optimisation can help encourage patient to take ownership of their treatment. To achieve the above we will process your personal data for the following purposes: • To conduct direct patient-facing activities on behalf of or at the request of a GP or General Practice. • To undertake analysis using specific criteria to identify individual patients that may benefit from a safer, more effective and / or more efficient medicinal regimes and approaches. This analysis may be conducted proactively or at the direct request of a General Practices and all lead to recommendations to the responsible clinician • To conduct administrative purposes which are necessary to ensure that the right payments are made, and staff are suitably trained to undertake the work safely and effectively **Legal Basis** – the legal basis below enables the ICB to process personal data for the purposes of medicines optimisation: Health & Social Care Act 2012 (Section 251b) (duty to share) NHS Act 2006 (Section 3a) (duty as to provision of certain services) GDPR Articles 6(1)(e) and 9(2)(h) **Benefits** – Frimley ICB can conduct Medicines Optimisation activities to ensure that patients receive prescribed items which are clinically effective and cost effective based on individual, local and national health population needs. We can also benchmark and share best practice at a practice level, locally and nationally to further improve our patients' experience of prescribed items and to the benefit of our local population. **Retention period –** The ICB will hold your information for a period of 5 years. Before records are destroyed, we will review information held and consider any further retention periods which may oblige us to hold the information for a further period.
Patient and Public Involvement	**Purpose** – 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 data which you have agreed to share with us.

	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. **Legal Basis** - Under the NHS Act 2006 Section 14Z2, the ICB has a duty, in relation to health services provided (or which are to be provided) under arrangements made by the ICB exercising its functions, to arrange for individuals to whom the services are being (or may be) provided are involved at various specified stages. We will rely on your explicit consent for this purpose. **Benefits** - If you would like to find out more information on how to get involved and how this benefits Frimley ICB, please see our Getting Involved pages. **Retention period** - Where you have provided us with your contact details for us to keep in touch, we will contact you periodically to ensure you are still happy for us to hold these details. If we do not hear back from you, we will delete your information from our database.
Clinical concerns, Quality monitoring and serious incidents	**Purpose** – Clinical Concerns was developed in response to the Francis Report 2013 and is a process through which the ICB works in collaboration with General Practices and other local healthcare Providers to gather intelligence about the quality and safety of local services and to facilitate learning and improvement. Your General Practice has appointed the ICB as the Data Processor to process Clinical Concerns on their behalf and have a Data Processing Agreement in place which identifies General Practice as the Data Controller and the ICB as the Data Processor. The Data Processing Agreement details the boundaries of sharing information and is reviewed on an annual basis. To facilitate the investigation of Clinical Concerns, your General Practice will provide the ICB with your NHS Number. The ICB will share this with the relevant healthcare providers involved in your care and treatment for them to investigate. The aim of this investigation is to resolve any outstanding issues in relation to the individual's care and treatment and to provide an opportunity to improve the quality of the service. The ICB will not use your NHS number for any other purpose. **Legal Basis** – The General Practice will rely on GDPR Articles 6(1)(e) and 9(2)(h) and the Health & Social Care Act (duty to share) as a legal basis to raise a Clinical Concern. The General Practice will provide you with comprehensive information by way of a Privacy Notice which clearly details the data sharing relationship with the ICB.

	The ICB will rely on the NHS Act 2006 Section 13R and 14Q as a legal basis to support their enactment of the following commissioning duties: • Information on safety of services provided by the health service • Duty as to effectiveness and efficiency • Duty as to the improvement in the quality of services **Benefits** - To assist with the gathering of intelligence about the quality and safety of local services and to facilitate learning and improvement. **Retention period -** The ICB will hold your information for a period of 10 years following the closure of a clinical concern. Before records are destroyed, we will review information held and consider any serious incident retentions which may require us to hold the information for a further period. Each case will be reviewed on an individual basis.
Commissioning, planning and contract monitoring	**Purpose** – To collect NHS data about services we have commissioned to provide services to you. We also work with other local ICBs and often hold joint contracts and commission joint services to make best use of the money available to us. We set our reporting requirements as part of our contracts with NHS service providers and do not ask them to give us identifiable data about you. **Legal Basis** - Our legal basis for collecting and processing information for this purpose is statutory under the Health & Social Care Act 2012, chapter A2 establishment and duties. **Data Processor and processing activities** – Hospitals and community organisations that provide NHS-funded care are legally and contractually obliged to submit certain information to NHS Digital about services provided to our service users. This information is 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. 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. 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. The specific terms and conditions and security controls that we are obliged to follow when using these commissioning datasets can also be found on the NHS Digital website. We also receive similar information from GP Practices within our ICB membership that does not identify you. **Benefits** - We use these datasets for several purposes such as: • 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. If you do not wish your information to be included in these datasets, even though it does not directly identify you to us, please contact your GP Practice and they can apply a code to your records that will stop your information from being included.
Primary & Secondary Care	**Purpose** – We commission a number of organisations to provide primary and secondary healthcare services to you. These organisations may be within the NHS or outside the NHS. Primary Care services cover GP Practices, Dental Practices, Community Pharmacies and high street Optometrists. Secondary Care services are usually (but not always) delivered in a hospital or clinic with the initial referral being received from Primary Care. These organisations may share identifiable, pseudonymised, anonymized, aggregated and personal confidential data information with us for the following purposes: • To look after the health of the public such as notifying central NHS groups of outbreaks of infectious diseases • To undertake clinical audit of the quality of services provided

	• To conduct risk profiling to identify patients who would benefit from initiative-taking intervention • To perform case management where the NHS offers intervention and integrated care programmes involving multiple health and social care providers • To report and investigate, complaints, claims and untoward incidents • To prepare statistics on our performance for the Department of Health • To review out care to make sure that it is of the highest standard **Legal Basis** - The Health & Social Care Act 2012 allows us to collect your information and is only accessed a limited number of authorised staff and not disclosed to other organisations. We will never share your personal information unless a legal basis has been identified for the different purposes of sharing or we have obtained your explicit consent. **Benefits** - Through sharing information ethically and lawfully the NHS can improve its understanding of the most important health needs and the quality of the treatment and care provided.
Risk Stratification	**Rationale** Risk stratification is a process that uses de-identified personal data from health care services to determine which people are at risk of experiencing certain outcomes, such as unplanned hospital admissions. **Data Processing activities for Risk Stratification** Risk stratification tools are used by ICBs to analyse the overall health of a population using data which is anonymised in line with the Information Commissioner's Office (ICO) Anonymization Code of Practice. The combined ICBs Secondary Use Service (SUS) data and GP data which contains an identifier (usually NHS number) is made available to clinicians with a legitimate relationship with their patients to enable them to identify which patients should be offered targeted preventative support to reduce those risks. The ICB has commissioned Graphnet to provide the risk stratification software solution on behalf of itself and its GP practices. This processing takes place under contract following the below steps: • NHS Digital has a legal obligation to obtain data from providers of NHS care such as the local hospital or community hospital. This data is then sent to the SCWCSU DSCRO and amended so that only your NHS number could identify you. The data is then provided to Graphnet for processing in the

	risk stratification software. The ICB has signed a Data Sharing Contract with NHS Digital for the use of this data, called Secondary Use Services (SUS) data. • Your GP practice enables an organisation called Graphnet Healthcare, to extract data from your records which again, is only identifiable by your NHS Number. This data will only be extracted and provided for those patients that have not objected to Risk Stratification or where no other type of objection to information sharing has been recorded on your record. The data, containing the same verified NHS numbers, are sent via secure transfer, to Graphnet. • Graphnet then link both sets of data using their risk stratification software. An algorithm is run on the data to generate a risk score for each Patient. The ICB can see data only after your NHS number has been removed and replaced by a pseudonymised reference. Your GP will be able to see the data with your NHS number in it so that it can identify if you require further support from them to manage your healthcare needs. The risk scores are only made available to authorized users within the GP Practice where you are registered via a secure portal managed by Graphnet. If you do not wish information about you to be included in the 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. Further information about risk stratification is available here. **Legal Basis** GDPR Art. 6(1) (e) and Art.9 (2) (h). The use of identifiable data by ICBs and GPs for risk stratification has been approved by the Secretary of State, through the Confidentiality Advisory Group of the Health Research Authority (approval reference (CAG 7-04)(a)/2013)) and this approval has been extended to the end of September 2020 NHS England Risk Stratification which gives us a statutory legal basis under Section 251 of the NHS Act 2006 to process data for risk stratification purposes which sets aside the duty of confidentiality. We are committed to conducting risk stratification effectively, in ways that are consistent with the laws that protect your confidentiality. **Benefits** ICBs and GPs use risk stratification tools as part of their local strategies for supporting patients with long-term conditions and to help and prevent avoidable admissions. 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. 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.
Infection Prevention and Control	**Purpose** - The ICB has an obligation for conducting Infection Control surveillances. This work is undertaken by a clinical nurse with support from Practices and Acute Trusts to provide the relevant information for the investigation to be undertaken and outcomes derived. **Legal Basis** - The Health Service (Control of Patient Information) Regulations 2000. Paragraph 3 enables the lawful processing of patient information in relation to diagnosing, recognising trends, controlling, preventing, monitoring and managing communicable diseases and other risks to public health. Mandatory Health Care Associated Infection Surveillance: Data Quality Statement April 2016 (PHE). **Benefits** The surveillance reports produce actions and lessons learnt that both support direct improved care of patients but also to continuously improve the safety of patients and be focussed on clinical learning. **Retention Period** - Post infection reviews may be kept up to eight years.
Learning Disabilities Mortality Review (LeDeR) Programme	**Purpose** - The Learning Disabilities Mortality Review (LeDeR) Programme aims to review the death of any person who lived with learning disabilities, identifying any health and social care factors relating to the death where things could have been done differently, and seeking to ensure that where care and treatment have not been at the expected standard this is not repeated elsewhere. The programme is co-ordinated by the University of Bristol in partnership with NHS England. The ICB participates in the programme by co-ordinating reviews at a local level. The LeDeR programme office (University of Bristol) can be told about the death of a person with learning disabilities by anyone holding that information. This could be, for example, a health or care professional, a relative, a service manager or another person with learning disabilities. When the death is notified to the programme, via a secure web portal, personal information about the person who has died is collected. This information is then shared with the ICB in the locality where the patient had been registered with their GP. The ICB co-ordinates the mortality reviews for its geographical area at the local

	level and is therefore privy to all the information about the case communicated from the LeDeR programme office. The information is communicated via a secure web platform. The ICB appoints a trained reviewer who then seeks further information about the person who has died from health or care professionals who have been involved in supporting that person. The reviewer may ask them questions about the health and care of the person, their diagnosis and treatments, and the circumstances leading up to their death. The reviewer may also need to look in the person's health or care records to check how their care was delivered. The reviewer will also make contact, when possible, with those closest to the person, including their families and/or carer, so that they can contribute to the review, should they wish. This will be done with the family and/or carer consent. The personal identifiable information collected for LeDeR reviews is uploaded, stored and communicated via a secure web platform hosted by the University of Bristol and covered by rigorous processes that meet NHS information governance requirements. • The information that the LeDeR programme gathers about people with learning disabilities who have died includes: • Personal details: (name, date of birth, date of death, gender, ethnicity, postcode, NHS number). These details help to identify the person who has died so that a local reviewer can trace their service contacts and conduct a review into their death. • Information about the circumstances leading to the person's death, which is held in health or social care records, to review the person's care, assess best practice and identify where service improvements may be required. • Information about the person's relative or next of kin (name, contact details, relationship), to invite them to contribute their views to the review. • Information about the person's cause of death. The central LeDeR programme office will share the NHS number (or any other information that could identify the person, e.g., date of birth and date of death) with NHS Digital. NHS Digital link this to information about cause of death held by the Office for National Statistics and send back to the LeDeR programme office the coding for the causes of death for people with learning disabilities whose deaths have been reviewed. Reports shared with local steering groups and other forums for the promotion of improvement and learning are shared in anonymised form with personal identifiers redacted.

	Legal Basis - The LeDeR Programme has obtained Section 251 approval from the Health Research Authority's Confidentiality Advisory Group (CAG 251), on behalf of the Secretary of State, allowing it to manage identifiable data without consent to conduct a review of a death, and to link it to NHS Digital cause of death data. The reference number for this is: 16/CAG/0056. CAG 251 allows data to be stored for the purpose of the programme for 10 years. **Benefits** - To make improvements to the lives of people with learning disabilities by identifying any potentially modifiable factors associated with a person's death and working to ensure that these are not repeated elsewhere. **Retention period** - Information relating to LeDeR reviews is retained by the University of Bristol for a period of 10 years from the completion of a review. The ICB will not retain personal identifiable information relating to reviews locally but will keep on file for 10 years anonymised review reports.
Assuring Transformation	**Purpose** - Assuring Transformation data is information we collect about people with a learning disability, autism or both who are getting care in hospitals for their mental health or because they have had behaviour that can be challenging. The ICB collects this data each month from healthcare Providers which is collected by NHS Digital. NHS Digital will publish a monthly progress report and provide this information to NHS England. These reports do not include any personal information. There is a calendar that tells you exactly when it will be published. This information informs NHS England of: • how many people are in hospital; • how long they have been in hospital for; • when their care and treatment is checked; • what kind of hospital they are in NHS England will check this information to make sure people are not in hospital if they would be better looked after in the community. NHS England has produced an Assuring Transformation Easy Read Leaflet which can be obtained from your healthcare Provider. **Legal Basis** - Assuring Transformation is a mandatory data collection of which has been approved by the Secretary of State under Regulations enabled by Section 251 of the NHS Act 2006 reference CAG 8-02(a-c)/2014. If you do not want your information to be included in these collections, please contact us.

	Benefits The published report allows the public to check if the NHS is doing a good job of looking after people with a learning disability, autism or both who are in hospital and assists NHS England in determining whether patients are getting the right care in the right place.
Cabinet Office	**Purpose -** The Cabinet Office is responsible for conducting data matching exercises. Data matching involves comparing computer records held by one body against other computer records held by the same or another body to see how far they match. This is usually personal information. Computerised data matching allows potentially fraudulent claims and payments to be identified. Where a match is found it may indicate that there is an inconsistency which requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is conducted. We participate in the Cabinet Office's National Fraud Initiative: a data matching exercise to assist in the prevention and detection of fraud. We are required to provide sets of data to the Minister for the Cabinet Office for matching for each exercise, as detailed here. **Legal Basis** The use of data by the Cabinet Office in a data matching exercise is conducted with statutory authority under Part 6 of the Local Audit and Accountability Act 2014. It does not require the consent of the individuals concerned under GDPR. Data matching by the Cabinet Office is subject to a Code of Practice. View further information on the Cabinet Office's legal powers and the reasons why it matches particular information here.
National Registries	National Registries (such as the Learning Disabilities Register) have statutory permission under Section 251 (16/CAG/0056) 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.
Research	**Purpose** – Data may be collected for the purpose of research. Research can be undertaken using information that does not identify you (anonymised). The law does not require your consent to be obtained in this case, but information should be made available to you where your anonymised data is used for the purposes of research. Information can be made available either in waiting rooms, using

	information leaflets, published on notice boards, waiting room screens and/or an organisations website. Where identifiable data is needed for research, you may be approached by an organisation who has provided you with care and asked if you wish to participate in a research study. Where identifiable data is required, an organisation must obtain explicit consent. A member of the research team will discuss the research study with you and will provide you with information on what the study is about, what information they wish to collect, how to opt out and who to contact for more information. If you do not wish your information to be used for research, whether identifiable or non-identifiable, please let your GP Practice know. They will add a code to your records that will stop your information from being used for research. **Legal Basis** – Your consent will be obtained by the organisation holding your records before identifiable information about you is disclosed for any research. If this is not possible then the organisation wishing to use your information will need to seek formal approval from the Confidentiality Advisory Group (CAG). For further information please visit the NHS Health Research Authority website. **Benefits -** Results from research studies can provide a direct benefit to individuals who take part in medical trials and indirect benefit to the population. **Retention Period** - Retention periods will be included in the research study Information Leaflet related to each study.
Employee Information	**Purpose and Legal Basis:** Frimley ICB processes information on the staff that it employs. The type of data processed includes personal information about staff including such data items as home addresses, NI number, date of birth as well as job related information such as salary, additional payments job titles and directorate. **Sources of employee information:** The ICB obtains information about our staff from the following sources: • Directly from staff; • From an employment agency; • From employers in the case of a secondee; • From referees, either external or internal; • From security clearance providers; • From Occupational Health and other health providers; • From Pension administrators and other government departments, for example, tax details from HMRC; • From the Trade Union. **What data does the ICB process and why:** Examples of what data the ICB holds and the reasons for holding it are as follows:

	Information related to employment We use the following information to conduct the contract we have with staff, provide staff access to business services required for their role and manage our human resources processes. We will also use it for our regulatory purposes in our role as a supervisory authority. • Personal contact details such as staff name, address, contact telephone numbers (landline and mobile) and personal email addresses; • Staff date of birth, sex and NI number; • A copy of staff passport or similar photographic identification and /or proof of address documents; • Marital status; • Next of kin, emergency contacts and their contact information; • Employment and education history including qualifications, job; • application, employment references, right to work information and details of any criminal convictions that staff declare; • Location of employment; • Details of any secondary employment, political declarations, conflict of interest declarations or gift declarations; • Security clearance details including basic checks and higher security, clearance details according to their job. • Any criminal convictions that staff declare to us. • Responses to staff surveys if this data is not anonymised. • Political declaration form in line with our policy and procedure regarding party political activities. **Information related to salary, pension and loans** We process this information for the payment of staff salary, pension and other employment related benefits. We also process it for the administration of statutory and contractual leave entitlements such as holiday or parental leave. • Information about job role and employment contract including start and leave dates, salary (including grade and salary band), any changes to employment contracts, working pattern (including any requests for flexible working). • Details of any time spent working and any overtime, expenses or other payments claimed, including details of any loans such as for travel season tickets. • Details of any leave including sick leave, holidays, special leave etc. Pension details including membership of both state and occupational pension schemes (current and previous). • Bank account details, payroll records and tax status information. • Trade Union membership for the purpose of the deduction of subscriptions directly from salary.

	• Details relating to Maternity, Paternity, Shared Parental and Adoption leave and pay. This includes forms applying for the relevant leave, copies of MATB1 forms/matching certificates and any other relevant documentation relating to the nature of the leave staff are taking. **Information relating to staff performance and training** We use this information to assess staff performance, to conduct pay and grading reviews and to deal with any employer/employee related disputes. We also use it to meet the training and development needs required for staff roles. • Information relating to performance at work e.g., probation reviews, PDRs, promotions. • Grievance and dignity at work matters and investigations to which staff may be a party or witness. • Disciplinary records and documentation related to any investigations, hearings and warnings/penalties issued. • Whistleblowing concerns raised by staff, or to which staff may be a party or witness. • Information related to staff training history and development needs. **Information relating to staff health and wellbeing and other special category data.** We use the following information to comply with our legal obligations and for equal opportunities monitoring. We also use it to ensure the health, safety and wellbeing of our employees. • Health and wellbeing information either declared by staff or obtained from health checks, eye examinations, occupational health referrals and reports, sick leave forms, health management questionnaires or fit notes i.e., Statement of Fitness for Work from GP or hospital. • Accident at work records. • Details of any desk audits, access needs or reasonable adjustments. • Information staff have provided regarding Protected Characteristics as defined by the Equality Act and s.75 of the Northern Ireland Act for the purpose of equal opportunities monitoring. This includes racial or ethnic origin, religious beliefs, disability status, and gender identification and may be extended to include other protected characteristics. **Lawful basis for processing staff personal data** Depending on the processing activity, we rely on the following lawful basis for processing staff personal data under the GDPR. • Article 6(1)(b) which relates to processing necessary for the • performance of a contract.

	• Article 6(1)(c) so we can comply with our legal obligations as an employer. • Article 6(1)(d) to protect staff vital interests or those of • another person. • Article 6(1)(e) for the performance of our public task. • Article 6(1)(f) for the purposes of our legitimate interest. **Special Category data:** Where the information we process is special category data, for example health data, the additional bases for processing that we rely on are. • Article 9(2)(b) which relates to conducting our obligations and exercising our rights in employment and the safeguarding of staff fundamental rights. • Article 9(2)(c) to protect vital interests or those of another person where staff are incapable of giving consent. • Article 9(2)(h) for the purposes of preventative or occupational medicine and assessing working capacity as an employee. • Article 9(2)(f) for the establishment, exercise or defence of legal claims. • Article 9(2)(j) for archiving purposes in the public interest. In addition, we rely on processing conditions at Schedule 1 part 1 paragraph 1 and Schedule 1 part 1 paragraph 2(2)(a) and (b) of the DPA 2018. These relate to the processing of special category data for employment purposes, preventative or occupational medicine and the assessment of working capacity as an employee. **Criminal convictions and offences.** We process information about staff criminal convictions and offences. The lawful basis we rely on to process this data are: • Article 6(1)(e) for the performance of our public task. In addition, we rely on the processing condition at Schedule 1 part 2 paragraph 6(2)(a). • Article 6(1)(b) for the performance of a contract. In addition, we rely on the processing condition at Schedule 1 part 1 paragraph 1. **How long we keep staff personal data** For information about how long we hold staff personal data, please see the Records Management Code of Practice for Health and Social Care 2016. **Data Sharing** In some circumstances, such as under a court order, we are legally obliged to share information. We may also share information about staff with third parties including government agencies and external auditors.

	For example, we may share information with HMRC for the purpose of collecting tax and national insurance contributions. Additionally, we are required under the Public Records Act 1958 (as amended) to transfer records to the National Archives (TNA) for permanent preservation. Some of these records may include the personal data of our current and former employees. Full consideration will be given to Data Protection and Freedom of Information legislation when making decisions about whether such records should be open to the public. **Does the ICB use any data processors?** Yes - a list of our current data processors can be found below: NHS South Central and West Commissioning Support Unit Omega House Southampton Road Eastleigh SO50 5BP Shared Business Services Phoenix House Topcliffe Lane Tingley Wakefield West Yorkshire WF3 1WE Health Assured Ltd The Peninsula Victoria Place Manchester M4 4FB Health Management Ltd Ash House The Broyle Ringmer Lewes East Sussex BN8 5NN **Employee rights in relation to this processing** Employees of the ICB have certain rights regarding our processing of their personal data, including a right to lodge a complaint with the Information Commissioner as the relevant supervisory authority. For more information on see your data protection rights. **Employee Vaccination Status – January 2022** The Health and Social Care 2008 (regulated activities) (amendment) (Coronavirus) (2.) Regulations 2022 require ICB staff to submit proof of vaccination to the ICB. This data will be processed by the ICB and

	authorised partners in confidence on a strictly need to know basis and is held for the ICB to comply with these regulations. Further information can be found about these regulations below: https://www.legislation.gov.uk/uksi/2022/15/made
Commissioning Support **South Central and West CSU** **NHS Digital DSCRO** **Optum Health Solutions (UK) Ltd**	**Purpose** - The ICB will use other organisations to provide us with support services. These organisations will process information on our behalf. These organisations are known as "data processors" and will provide additional expertise to support the work of ICB: **Legal Basis** - The ICB are committed to ensure that a legal basis is identified for all flows of personal identifiable to external organisations. The ICB ensures that this is supported by use of an NHS Standard Contract which is mandated by NHS England for use by commissioners for all contracts for healthcare services other than primary care. **Activities** – Undertakes the processing of pseudonymised SUS data and local data flows to provide contract management for the services commissioned by the ICB, other than those identified above with the applicable legal basis Legal Basis - GDPR & Data protection Act, S251 NHS Act 2006 & Health and Social Care Act 2012 **Activities** – Undertakes the processing of identifiable Secondary Use Service (SUS) data and local data flows to provide pseudonymised commissioning data to the ICB's 'processors'. **Legal Basis** - NHS Act 2006 & Health and Social Care Act 2012 Activities - Undertakes the processing of pseudonymised SUS data and local data flows to provide contract management for London Providers commissioned by the group known as The London Focus Group Legal Basis - GDPR & Data Protection Act, S251 NHS Act 2006 & Health and Social Care Act 2012
Other organisations who provide support services for us	**Purpose** -The ICB will use the services of additional organisations (other than those listed above), who will provide additional expertise to support the work of the ICB. **Legal Basis** - We have entered into contracts with other organisations to provide some services for us or on our behalf. These organisations may process or be in the vicinity of ICB data and could be identified as 'processors'. Information that we may hold about people will not be shared or made available to any of these organisations. Below are their details and a brief description of the functions they conduct on our behalf: TIAA & PWC – Provide internal audit services for the ICB Grant Thornton – Provide external audit services for the ICB

	PHS Records Management – For storing archived records For further details, please contact the ICB.