



## **SHELLEY MANOR & HOLDENHURST MEDICAL CENTRE**

### **EMPLOYEE AND APPLICANT PRIVACY NOTICE**

#### [Covid-19 testing programme for staff](#)

##### **Why is this programme taking place?**

A voluntary antibody testing programme has been commissioned by the Department of Health and Social Care (DHSC) for critical workers and their household members who are self-isolating because they are showing symptoms of Covid-19. DHSC are the data controller for the programme and a copy of their privacy notice can be found [here](#). Samples are tested in local laboratories and the results are recorded in a database called the local Integrated Clinical Environment (ICE) database. Access to this database is strictly controlled and audited and can only be accessed for clinical reasons by clinical staff caring for you. You do not need to tell us if you test negative. You will need to tell us if you test positive as you will need to self-isolate, and if it is confirmed that you have contracted Covid-19 through exposure at work, we are obliged to report this to the Health and Safety Executive.

#### [Covid-19 antibody testing programme for staff](#)

##### **Why is this programme taking place?**

A voluntary antibody testing programme for NHS staff is being carried out at the request of NHS England and NHS Improvement to provide information on the prevalence of Covid-19 in different regions of the country and help better understand how the disease spreads. Covid-19 is a new disease and our understanding of the body's immune response to it is limited. The benefit of processing this information is that it will enable understanding of the virus to grow as new scientific evidence and studies emerge. If you choose to take part in the programme, you will learn whether you have had the virus that causes Covid-19 in the past and whether you have developed antibodies to the virus. The research into the prevalence of Covid-19 will enable the Practice to develop infection control measures and safe working practices for the future.

##### **What information will be collected?**

If you consent to take part in the programme you will be provided with information about the programme and a consent form. The personal and special category data collected from you on the consent form will include date of the blood test, name, mobile phone number, NHS number, ESR number, job role, ethnic group, health details relating to whether you believe you have had Covid-19, the symptoms experienced and whether you have been hospitalised, and whether you are on any immunosuppressant medication and the drug details if applicable.

##### **Lawful basis**

The lawful basis for the testing and sharing of your personal data with the Practice and your registered GP under UK GDPR is Article 6(1)(e) processing is necessary in order to protect the vital interests of the data subject or of another natural person.

The additional condition for processing special category health data under UK GDPR is Article 9(2)(g) processing is necessary for reasons of substantial public interest, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

The lawful basis for sharing personal information nationally and with the Covid-19 research programme is the Notice under Regulation 3(4) of the Health Service Control of Patient Information Regulations 2002 issued by the Secretary of State for Health and Social Care 20/03/20 (COPI).

### **Who will your information be shared with?**

Results will be shared with the Practice, your GP, Public Health England and other NHS providers for Public Health and Healthcare purposes. The anonymised result will also be reported as part of national reporting requirements. Some or all personal information may also be shared with a Covid-19 research programme to held in the search for a treatment and vaccine for Covid-19.

### **How long will this information be kept for?**

The Practice will keep a record of all staff, whether they have been tested and whether the result was positive. This documentation will be retained by the Practice for *[insert details]*. It is possible that this record will become a 'record of historical importance' – if this is the case it will be retained by the Practice for 20 years, after which transfer to a local place of deposit will be considered.

Test results will be shared with your registered GP who will enter them into your health record and retain in accordance with the retention schedule set out in the NHS Records Management Code of Practice 2021.

## **Homeworking**

### **Access to SystemOne**

Staff may be asked to work from home during the current Coronavirus Outbreak. Where this is the case, access to medical records on SystemOne will continue to be monitored and audited in the same way as it is when staff are working on Practice premises. Staff should only access medical records where there is a legitimate reason to do so. Any unauthorised access to records will be investigated in accordance with the Practice disciplinary procedures.

## Tier One – Overview of information held and shared

This Privacy Notice explains and describes how this GP Practice uses and manages the information it holds about its staff and job applicants. This includes how the information may be shared with other NHS organisations and with non-NHS organisations, and how the confidentiality of information is maintained.

### Our contact details

Organisation Name	Shelley Manor & Holdenhurst Medical Centre
Address	Beechwood Avenue, BH5 1LX 199 Holdenhurst Road, BH8 8DE
Phone number	01202 587111 or 01202 309421
Email	smh.mc@nhs.net
Data Protection Officer	Helen Williams/Emily Hutchings Dorset CCG
Data Protection Registration Number	Z6866012

### What type of information do we hold about job applicants?

We collect and process the following information about job applicants:

- personal contact details – name, address, contact telephone number(s), email address, gender;
- employment and education history including your qualifications, skills, experience, membership of any professional bodies, employment references and details of any criminal convictions that you declare;
- a copy of your passport or similar photographic identification and / or proof of your current address;
- information about your current level of remuneration, including benefit entitlements;
- whether or not you have a disability for which the Practice needs to make reasonable adjustments during the recruitment process;
- details about your health including any medical needs or conditions;
- details of any pre-employment assessments;
- information about your entitlement to work in the UK;
- equal opportunities monitoring information including information about your ethnic origin, sexual orientation, health and religion or belief.

The Practice collects this information from a number of sources, such as:

- application forms;
- CVs or resumes;
- copies of your passport and other identity documents;
- interview notes or notes from other forms of assessment;
- information from correspondence with you.

We are required to obtain this information about you to comply with employment law in order to assess your capacity to work, to ensure that equality law is being met through the recruitment process and to comply with any safeguarding laws relating to the role you are applying for. You are under no statutory or contractual obligation to provide data to the Practice during the recruitment process. However, if you do not provide the requested information, the Practice may not be able to process your application.

### **Sharing job applicant information**

Your information will be shared internally for the purposes of employment. This includes:

- interviewers involved in the recruitment process;
- GPs and Practice Manager.

If you are successful in your application, the Practice will also share your data with former employers and nominated individuals in order to obtain references for you carry out employment background checks with providers, and obtain necessary criminal records checks through the Disclosure and Barring Service (DBS).

### **What type of information do we hold about our staff?**

We collect and process the following information about our staff:

- identity details – name, date of birth, gender, nationality, NI number;
- images (whether captured on CCTV, by photograph or video);
- personal contact details – address, contact telephone number(s), email address;
- a copy of your passport or similar photographic identification and / or proof of your current address;
- details about your marital status, 'next of kin' or emergency contact information;
- employment and education history including your qualifications, job application, employment references, right to work information and details of any criminal convictions that you declare;
- Disclosure Barring Service (DBS) criminal record check details where necessary for the job role;
- information about your job role and employment contract including start/leave dates, salary, any changes to your employment contract, working patterns and any requests for flexible working or changes to employment, and location of employment;
- performance at work documents such as probationary reviews, appraisals and any training or development you have undertaken;
- grievance and dignity at work records and investigations, disciplinary records and documentation, incident investigations and statements where you are involved;
- accident records, workplace assessments, access needs assessments and reasonable adjustment documentation;



- medical and health conditions, immunisation records if appropriate for your role, and details you have provided about protected characteristics;
- details of time spent working, including overtime, expenses and other claimed payments;
- details of leave including sick leave, holidays, special leave, sabbaticals and career breaks;
- pension details, bank account details payroll records and tax status information;
- details relating to maternity, paternity, shared parental / adoption leave and pay applications for the relevant leave, copies of MATB1 forms/matching certificates and other relevant documentation;
- details relating to your car insurance and registration for parking and mileage claims;
- details of trade union membership, and equal opportunities monitoring information including information about your ethnic origin, sexual orientation, health and religion or philosophical belief.

The Practice collects this information from a number of sources, such as:

- directly from you;
- from an employment agency;
- application forms;
- CVs or resumes;
- copies of your passport and other identity documents;
- interview notes and any assessment information;
- from referees, either external or internal;
- from security clearance providers;
- from pension administrators and other government departments, for example tax details from HMRC;
- CCTV images from our landlords or taken using our own CCTV systems;
- from Occupational Health and other health providers;
- information provided by you or generated about you during the course of your employment.

You are required under your employment contract to provide some information to the Practice, such as absences from work, annual leave requirements, information about disciplinary or other matters. Failure to provide this information may mean that you are unable to exercise your statutory rights.

### **Sharing staff information**

Your information will be shared internally for the purposes of employment. This includes:

- line managers and Human Resources;
- finance and payroll;

- Practice Manager or team members with responsibility for health and safety including first aid, accidents, incident investigations and complaints.

### **Other organisations we share with**

The Practice shares and receives employee information from a range of organisations or individuals for a variety of lawful purposes, including:

- NHS Jobs and other employment agencies;
- Occupational Health;
- Payroll, HMRC;
- NHS Pensions;
- CCG for reimbursement of salaries under DES contract;
- CCTV providers;
- IT staff;
- your employer or place of work if you are a secondee or a contractor;
- any new employer under TUPE or where a reference is requested;
- disclosure to bodies with statutory investigative powers e.g. the Care Quality Commission, the GMC, the Audit Commission and Health Services Ombudsman;
- NHS England;
- emergency services in the case of an emergency.

Employee information is only shared with other organisations when there is a legal basis to do so, such as:

- where there is a contract in place for data processing;
- where there is a Court Order or statutory duty to share information;
- where there is a statutory power to share information;
- where the employee has given explicit consent to the sharing of information.

Employee information is only shared on a need to know basis when there is a direct reason to do so, and is limited to what is necessary for that purpose such as providing employment rights and payroll.

### **Tier Two – Purposes of processing, retention and your rights**

#### **Purposes of processing**

Our Practice processes employee and job applicant data in order to meet our statutory legal obligations, to provide employment and an employment contract, to check your entitlement to work in the UK and whether you have any criminal convictions, to pay you and manage benefit, pension and insurance entitlements in accordance with your employment contract. We keep records in order to have accurate and up to date information available to ensure that employee rights and remuneration are in place. Our Practice values the concept of data minimisation and uses anonymous or pseudonymised data where possible.

Your data will be stored in a range of different places, including your personnel file, and HR, email and IT systems e.g. Bright HR, TeamNet.

We do not process the information of unsuccessful job applicants but your information may be retained for future opportunities. Please see section on retention.

### **Primary Care Networks**

Primary Care Networks (PCNs) are groups of GP Practices working closely together with their local partners (e.g. other primary and community care staff, mental health, social care, pharmacy, hospital and voluntary services) for the benefit of patients and the local community. Our Practice is part of Bournemouth East Collaborative Primary Care Network, alongside Southbourne Surgery, Littledown Surgery and Beaufort Road Surgery.

Your information (name, clinics and working hours) may be seen by employees from anywhere in our PCN, at any of the Practices, in order for our PCN administrators to be able to view clinics and book appointments.

### **Primary Care Web Tool**

Practices are required to make national quarterly returns to NHS England via the primary Care Web Tool system. This is a submission to support a national record of the primary care workforce.

### **Dorset integrated care system (ICS)**

Dorset's integrated care system, known locally as 'Our Dorset' is a partnership of local organisations (health and local councils) working together to improve services to meet the needs of local people and deliver better outcomes. Our Dorset have a Dorset Intelligence and Insight (DiiS) Business Intelligence platform which uses pseudonymised data to reveal important insights into local and community healthcare, in order to inform the future of healthcare for communities. In order to effectively manage new services, pseudonymised employee information is also shared into the DiiS in order to assess the workforce requirements.

### **Other ways in which staff or applicant information may be used:**

#### **Incident management**

If you are involved in an incident, for example you slip and fall whilst in the Practice, your information may be included in the incident report and used as part of the investigation process.

#### **Emails**

In the event of staff absence/annual leave, we may need to access your emails held on our Practice email system in order to deal with correspondence and to ensure business as usual. Personal emails must therefore be marked as personal and private to distinguish between

work and private matters in the emails. We may also need to search email in and sent boxes to assist with disciplinary investigations. Emails will be accessed following a request to our IT support team. In the event of you leaving the Practice, we will arrange for all emails sent to your inbox to be forwarded to your line Manager, for business continuity purposes.

### **Recorded telephone calls**

We record a selection of incoming and outgoing telephone calls to and from the Practice to assist with training, for patient telephone consultations, for medic-legal purposes and for quality assurance and responding to complaints. Recordings of telephone calls will only be accessed where necessary by the Practice management team. We may also record meetings attended remotely by Practice staff using MS Teams. We store recordings in accordance with the NHS Records Management Code of Practice 2021, after which they are deleted.

### **Complaints and queries**

If a complaint or query is raised with the Practice which requires your involvement, we may obtain statements from you and/or conduct interviews with you and hold that information within a secure database in order to ensure that the complaint or query can be answered appropriately. Details of complaints or queries will not be stored within your employment records.

### **Secondary uses**

We may also process data for the following secondary uses:

- **Risk stratification and population health management:** we use the services of analytics staff in Dorset Healthcare as part of the Intelligent Working Programme (IWP) to pseudonymise and extract data and transfer it to analytics staff at Optum for linking with Secondary Uses data with the aim of improving short term and medium term health outcomes for local populations through the application of Population Health Management. Pseudonymised patient data and staffing and vacancy levels are used to allow Dorset the opportunity to plan and sufficiently staff future services.
- **National archiving:** records made by an NHS organisation are Public Records in accordance with Schedule 1 of the Public Records Act 1958. The Public Records Act 1958 requires organisations to select core records for permanent preservation at the relevant Place of Deposit (PoD) appointed by the Secretary of State for Culture, Media and Sport. PoDs are usually public archive services provided by the relevant local authority. Records no longer required for current service provision may be temporarily retained pending transfer to a PoD and records containing sensitive personal data should not normally be transferred early.
- **Improving Services:** pseudonymised workforce information is sometimes used to help assess the workforce requirements when identifying areas for improvement in the services provided to our communities.



These secondary uses of data help the NHS to meet our statutory obligations under the Public Records Act 1958, and to plan and manage health services for the population of Dorset.

### **Data controller and processors**

The Practice is the data controller of the data we gather, hold and create about you. We engage with data processors who may process your data. All data processors are held to strict contractual obligations which specify the limitations, any access arrangements, storage and retention of data on our behalf as well as strict confidentiality and information handling clauses. All data processors are also held to high information security standards and are asked to provide evidence of how they meet data protection legislation. These processors may be software suppliers or specialist and support services.

### **Cross Border Transfers between the UK, the EU, other third countries or international organisations**

Following the UK's exit from the European Union the UK has now become a third country under the EU GDPR. An adequacy decision for the UK has been approved by the EU Commission under Article 45(3) of the EU GDPR, allowing the free flow of personal data between the EU and the UK to continue. The Practice does not routinely transfer data outside of the European Economic Area and will assess any adhoc transfers against adequacy (UK GDPR Article 45) and appropriateness of safeguards and data protection (UK GDPR Article 46) of the country of transfer.

### **Retention periods**

The Practice works to the NHS Records Management Code of Practice 2021 Retention Schedule: [Records Management Code of Practice 2021 - NHSX](#)

#### **Employee retention:**

As a standard we will retain your full employment record for 6 years, after which it will be condensed to a summary and retained until your 75<sup>th</sup> birthday, or 6 years after if you are over 75 years of age.

#### **Applicant retention:**

Job applications and adverts are retained on NHS Jobs for up to 460 days after the closing date, depending on the relevant closing date for the advert, and then deleted. An audit log will be retained for 24 months to allow processes to be independently checked. If you have applied for a position via an alternative employment agency, they will be able to provide you with their own privacy notice. We will retain all candidate applications for 12 months, in the event of another position arising that we wish to offer you. After such a time we will securely dispose of your information.

## Data subject rights

The law gives you certain rights in relation to the personal information that we hold about you:

### 1. Right of access to your information

You have the right to request a copy of the personal information that we hold about you by contacting the Practice Manager. We will provide this information, within one month, free of charge. We can restrict disclosure of your information if we feel that granting access would disclose information likely to cause serious harm to your physical/mental health, or that of another individual, and you do not already know the information. Or where access would disclose information about/provided by a third party who could be identified from the information and who has not consented for it to be released.

### 2. Right to restrict or object to the use of your information

We cannot share your information with anyone else for a purpose that is not directly related to your employment or a statutory requirement without your consent. If you wish to restrict or object to the use of your information, you should contact our Practice Manager.

### 3. Right to have incorrect information corrected

If you feel that the information we hold about you is incorrect, you have the right to ask for it to be corrected. This applies to matters of fact, not opinion. Incorrect contact information will be corrected immediately.

### 4. Right to data portability

This right only applies where the original processing is automated and is based on your consent or fulfilment of a contract that you are party to. In the spirit of the Regulation, you can request that your personal information is transferred in an electronic or other form to another organisation.

### 5. Right to appropriate decision making

The right to appropriate decision making applies to automated processing, including profiling, which produces legal outcomes, or that significantly affects you. The Practice has not identified any automated processing which is solely automated and without human involvement in the outcome of the decision.

### 6. Right to erasure

This is sometimes known as 'the right to be forgotten', but it is not an absolute right. You cannot ask for this right in relation to records which the Practice is legally bound to retain. The Practice has an obligation not to retain information for longer than is necessary and to dispose of information securely.

## 7. Right to lodge a complaint

If you are dissatisfied with the handling of your personal information, you have the right to make a complaint. In the first instance, formal complaints should be addressed to the Practice Manager.

You also have the right to make a complaint to the Information Commissioner's Office (the independent regulator of data protection) by using their online submission form

<https://ico.org.uk/global/contact-us/> or by writing to:

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

### Tier Three – The law explained

#### Data Protection Principles

There are six core principles to data protection legislation:

1. Personal data must be processed lawfully, fairly and transparently (lawfulness, fairness and transparency).
2. Personal data must be collected for specific, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes (purpose limitation).
3. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).
4. Personal data must be accurate and up to date (accuracy).
5. Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation).
6. Personal data is processed in a manner that ensures appropriate Security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).

#### Lawful basis

The Practice relies on the following lawful bases for processing your personal data under the UK GDPR and for processing information about staff criminal convictions and offences:

- **Article 6(1)(b):** "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"

- **Article 6(1)(c):** “processing is necessary for compliance with a legal obligation to which the controller is subject”
- **Article 6(1)(e):** “processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.”

The Practice must operate in accordance with UK legislation such as the National Health Service Act 2006, the Health and Social Care (Safety and Quality) Act 2015, Equality Act 2010, Health and Safety at Work Act 1974, Transfer of Undertakings (Protection of Employment) Regulations 2006, the Crime and Disorder Act 1998, Terrorism Act(s), Children's Act(s) 1989 and 2004, Mental Health Act 1983 and 2007.

Where the information we process is special category data, the additional bases that we rely on for processing under the UK GDPR are:

- **Article 9(2)(b):** “Processing is necessary for the purposes 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.”
- **Article 9(2)(f):** “Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.”
- **Article 9(2)(h):** “Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health and social care systems and services.”
- **Article 9(2)(i):** “Processing is necessary for reasons of public interest in the areas of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.”
- **Article 9(2)(j):** “Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.”

Where data has been anonymised it is not considered to be personal data and the UK General Data Protection Regulation 2016/679 and Data Protection Act 2018 will not apply.

Our Practice upholds transparency and fairness through the use of this privacy notice. We uphold data minimisation techniques like pseudonymisation and anonymisation where possible to protect data and ensure that the purpose of processing is relevant and adequate. The Practice holds data security in the highest importance; our systems have role-based access and clinical systems are auditable to ensure transparency in the use of systems by staff. Devices are encrypted and all our staff undertake annual mandatory data security training. Where we hold paper records, these are held securely in a locked filing cabinet in a locked office. Internal policies and controls are in place to protect your information.