**Atholl Medical Centre Patient Privacy notice**

**WHAT IS THE PURPOSE OF THIS DOCUMENT?**

|  |
| --- |
| Atholl Medical Centre is committed to protecting the privacy and security of your personal information.  This privacy notice describes how we collect and use personal information about you during and after your patient relationship with us, in accordance with the General Data Protection Regulation (GDPR) and Data Protection Act 2018.  It applies to all patients registered with the practice in a permanent or temporary category |

Atholl Medical Centre is a “data controller”. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

**DATA PROTECTION PRINCIPLES**

|  |
| --- |
| We will comply with data protection law. This says that the personal information we hold about you must be:  1. Used lawfully, fairly and in a transparent way.  2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.  3. Relevant to the purposes we have told you about and limited only to those purposes.  4. Accurate and kept up to date.  5. Kept only as long as necessary for the purposes we have told you about.  6. Kept securely. |

**THE KIND OF INFORMATION WE HOLD ABOUT YOU**

|  |
| --- |
| Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).  There are “special categories” of more sensitive personal data which require a higher level of protection.  **We collect your personal details and hold your medical records so that we can provide you with the healthcare service you have requested of us by joining our Surgery.** |

We may collect, store, and use the following categories of personal information about you:

1. Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
2. Date of birth and CHI number (a NHS Scotland identifier unique to each individual)
3. Gender.
4. Marital status and dependants.
5. Next of kin and emergency contact information.

Due to the nature of our business we may also collect, store and use the following “special categories” of more sensitive personal information:

1. Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
2. Information about your health, including any medical condition, health and sickness records.
3. Genetic information and biometric data.
4. Information about criminal convictions and offences.

**HOW IS YOUR PERSONAL INFORMATION COLLECTED?**

We collect personal information on our patients through the registration process. This information is freely provided by yourself or a parent/guardian. Your medical record information is built up from the time of your birth and contains information accrued in various ways:

* Details gathered during consultations; in person or on the phone
* Letters from other healthcare providers regarding their care of you
* Letters from other professional bodies;eg Insurance companies, Government departments and Police

Medical Records of patients joining our Practice from another practice are sent to us by the NHS Medical records holding authority- Practitioner Services Scotland. These records are only sent to us after we have sent them a registration document which has been filled out by yourself or parent/guardian.

**HOW WE WILL USE INFORMATION ABOUT YOU**

|  |
| --- |
| We only collect and use your personal information as the law allows us to. The Lawful Bases for processing your data we pertain to under the new GDPR guidelines is: ‘Processing is required for compliance with a legal obligation the Data controller is subject to’. We are allowed to use the special category data we hold on you for this reason - Healthcare, occupational health and public health and safety.  Most commonly, we will use your personal information in the following circumstances:  1. Where we need to perform the contract we have entered into with you eg Your healthcare  2. Where we need to comply with a legal obligation eg Procurator Fiscal medical record requests  3. Completion of Insurance company or Solicitor Medical Records reports which will have first been consented for completing by yourself.  We may also use your personal information in the following situations, which are likely to be rare:  1. Where we need to protect your interests (or someone else’s interests).  2. Where it is needed in the public interest [or for official purposes]. |

**SITUATIONS WHERE WE WILL USE AND/OR SHARE YOUR PERSONAL INFORMATION**

We need all the categories of information in the list above (see [*The kind of information we hold about you*](#co_anchor_a486023_1)) primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we must give your personal information to third parties so they can continue with the job of providing you with necessary healthcare. The Surgery has a file and policy which details the means we use your data for and how it is protected when shared with 3rd parties. You can ask to see this on request but below is a summary of what we most regularly do with your data, who we share it with and how we protect it:

1. Surgery staff Clinical consultations. Clinical software is password protected and backed up daily. Backed up data is encrypted and only accessible through the clinical software.
2. Referring you to Secondary Care Healthcare providers. Information given will include personal contact information and medical record information pertaining to the referral (this can sometimes include photographs eg dermatology referrals). These referrals are made on an electronic system maintained by NHS Tayside which is password protected and has rigorous Firewall controls.
3. Processing of Prescriptions. Prescriptions are kept secure in our back office which is protected by a security door. Prescriptions are delivered in person to the Pharmacy who process them according to their own data policy which will be GDPR compliant.
4. Checking upon registration that you are legally entitled to healthcare in the UK
5. Contacting you via the personal information you have provided to inform you of: upcoming appointments, test results and other matters directly related to your healthcare. This information is secure if you ensure you update of us of any changes to your personal information.
6. Completing Insurance reports requested by Insurance companies on behalf of yourself. These reports are either completed on a secure IT platform that both the Insurance company and the Surgery both use; or they are completed by hand and posted back to the company. All letters are marked Private and Confidential.
7. Medical record requests from Solicitors on behalf of yourself. These can be reports or your entire Medical record depending on the requirements. We are legally obliged to provide the records to the Solicitor in the form they request, this can mean copies of your records being posted out. To ensure greater protection request that your solicitor requests your records as a password protected document file which we email to them.
8. The Police and procurator fiscal can make requests to see your Medical Records we can decide whether these requests are justifiable. Again ideally we send these as password protected document files.
9. Anonymised healthcare data is shared with the Health Board and Government for the purpose of proving we are upholding our end of the healthcare contract we have entered into with yourself, and as a business with NHS Scotland.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

We will only share your information with 3rd parties with your consent or where we have a legal obligation to do so and we will make the best means available to protect your data during the sharing process.

**If you fail to provide personal information**

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you, which is providing you with healthcare. Or we may be prevented from complying with our legal obligations.

**Change of purpose**

**We will only use your personal information for the purposes for which we collected it.**

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Otherwise the sharing of your personal details will be for your benefit only. For the furtherance of your Healthcare and to aid in any activities you the patient have entered into and have consented for your data to be shared for the purpose of successfully pursuing these activities eg Insurance claims, Benefits claims

**HOW WE KEEP YOUR DATA SECURE**

|  |
| --- |
| The personal data we hold on you is stored within our Clinical Systems: Vision and Docman. Data can then be transferred for the purpose of referrals through another Clinical System called SCI-Gateway which is hosted by the health board. All these clinical systems are password protected and all staff are aware of our Data Protection Policy and the penalties for misuse of data.  Hard copies of personal data: Paper medical records, prescriptions and correspondence from other professions are kept securely in our back office which is protected by a security door. All correspondence we receive pertaining to a patient is scanned directly into the electronic medical record of the patient and upon verification that the clinical system has successfully completed its daily backup is shredded on-site.  The clinical system back-ups are done in an encrypted form onto back-up tapes. These tapes are rotated daily and protected until the next back-up via a fire retardant safe. Therefore protecting your data against breaches but also from it getting deleted/destroyed.  We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so. |

**HOW CAN YOU ACCESS THE DATA WE HOLD ON YOU**

Under the new GDPR regulations we as a Practice have to comply with all ‘reasonable’ requests from patients to access the data we hold on them. These are called Subject Access Requests (SARs). You can make these requests directly yourself to the Practice or independently through a solicitor or nominated 3rd party (for those types of requests we need to have your consent verified first). The term ‘reasonable’ is to be interpreted by the business, in our case it would be used in relation to frequency of these requests. For example monthly requests to have a printed copy of your Medical records would certainly be deemed ‘unreasonable’.

Ideally we would opt to share your Medical Record with you as a password protected document file we email to you.

The new Data laws do still allow a GP to refuse patient access to medical records if this could be considered harmful to the patient.

Any SAR request you make doesn’t have to include your medical record. You may just wish to know what personal data we hold on you as opposed to Special category data like your medical record.

Our Data Protection Officer is our Practice Manager. If you wish to make a SAR please contact them.

**DATA SHARING**

|  |
| --- |
| We do have to share your data with third parties, including third-party service providers and other entities in the group.  We require third parties to respect the security of your data and to treat it in accordance with the law. |

**Why might you share my personal information with third parties?**

We may share your personal information with third parties where required by law, where it is necessary to administer the healthcare relationship with you or where we have another legitimate interest in doing so.

**Which third-party service providers process my personal information?**

Secondary care departments we have referred you to, these departments will have their own patient privacy policies available through the Health Board. They will use your information to contact you with appointment information and results. Without access to your personal information they would not be able to proceed with your referral.

**How secure is my information with third-party service providers and other entities in our group?**

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for purposes beyond your healthcare. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

**What about other third parties?**

We may also need to share your personal information with a regulator or to otherwise comply with the law. We will also share your personal information at your request with whomever you specify should have it.

**Transferring information outside the EU**

We **do not** envisage having to share your information with 3rd Parties outside the EU but will notify you if our position changes

**DATA RETENTION**

**How long will you use my information for?**

In Scotland, GP Surgeries are to retain the Paper Medical Records of patients for their entire lifetime with the practice and for 3 years after their death.

However in the case of electronically stored medical records these are currently not allowed to be destroyed or deleted for the foreseeable future.

**RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION**

**Your duty to inform us of changes**

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your healthcare relationship with us.

**Your rights in connection with personal information**

Under certain circumstances, by law you have the right to:

1. **Request access** to your personal information (commonly known as a “subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
2. **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected. This does not relate to Medical Records.
3. **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
4. **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
5. **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
6. **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Practice Manager in writing.

**No fee usually required**

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

**What we may need from you**

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

**RIGHT TO WITHDRAW CONSENT**

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Data Protection Officer c/o Atholl Medical Centre. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

If you withdraw consent it may interfere or stop us being able to provide Healthcare to you at a standard our GPs consider adequate. In that case we may request to have you removed from our list.

**DATA PROTECTION OFFICER**

We have appointed a data protection officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO c/o Atholl Medical Centre. You have the right to make a complaint at any time to the Information Commissioner’s Office (ICO), the UK supervisory authority for data protection issues.

**CHANGES TO THIS PRIVACY NOTICE**

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.