Defence Primary Healthcare and SSAFA
PATIENT PRIVACY NOTICE

This privacy notice lets you know what happens to any personal data that you give to us, or any that we may collect from or about you and explains how we collect and process this to meet our obligations to you.
This privacy notice applies to your personal data processed by or on behalf of Defence Primary Healthcare (DPHC)

YOUR RIGHTS

- To be Informed – Privacy Notice
- Access – Subject Access Request
- Rectification – Incorrect or incomplete information amended
- Restrict Processing – if validity is contested restrict use of information.
- Object – to how your information is processed (i.e. marketing or research)
- Erasure – deletion or removal where there is no compelling reason for processing
- Data Transfer (Portability) – provide data in a format you can use

PATIENT PRIVACY NOTICE:

1. Introduction

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA18) form the legal framework for protecting your Personal Data.
We will comply with the data protection principles set out in the GDPR. These say that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way;
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date;
- Kept in a form which permits you to be identified only as long as necessary for the purposes we have told you about;
- Kept securely.

The Ministry of Defence is the data controller for all personal data that we hold about you. Contact details are in section 13 of this Notice.

In DPHC, we are committed to protecting your privacy and will only use personal data collected lawfully in accordance with:

Data Protection Act 2018	Caldicott Principles
General Data Protection Regulation	Common Law Duty of Confidentiality
Access to Health Records Act 1990	MOD Joint Service Publications (JSPs)
Health and Social Care Act 2015	NHS Codes of Confidentiality
Human Rights Act 1998	Information Sharing Principle – To Share or Not to Share Review

2. The personal data we collect and use

When you register with a DPHC facility we must collect basic '**personal data'** about you. This includes your name, address, contact details such as email and mobile phone number. We will also ask you for health information which is known as **'Special category data'**. We are required to do this to ensure your healthcare information is linked between other healthcare providers that may be required to help in the delivery of your care.
We will also collect the following types of information from you or about you from a third party, for example a hospital or healthcare professional organisations:

- Details about you such as your address, legal representative, emergency contact details;
- Any contact the healthcare organisation has had with you, such as appointments, clinic visits, emergency appointments, etc.;
- Notes and reports about your health;
- Details about your treatment and care;
- Results of investigations such as laboratory tests, x-rays etc.;
- Relevant data from other health professionals, relatives or those who care for you.

3. Our legal basis for processing your personal data

The legal basis under which we process your personal data (including special category data) is as follows:

- 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 MOD;
- Article 6(1)(c) – processing is necessary for compliance with a legal obligation;
- Articles 6(1)(d) and 9(2)(c) – processing is necessary in order to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- 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 or social care systems and services;
- Article 9(2)(i) – processing is necessary for reasons of public interest in the area of public health;
- Article 9(2)(j) – processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

The Ministry of Defence may also process personal data for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings), for the purpose of obtaining legal advice, or for the purpose of establishing, exercising or defending legal rights.

Where we process personal data for these purposes, the legal basis for doing so is:

- 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 MOD; or
- Article 6(1)(c) – processing is necessary for compliance with a legal obligation to which the MOD is subject; or
- Article 6(1)(f) – processing is necessary for the purposes of legitimate interests pursued by the MOD.

Where we process special categories of personal data for these purposes, the legal basis for doing so is:

- Article 9(2)(f) – processing is necessary for the establishment, exercise or defence of legal claims; or
- Article 9(2)(g) – processing is necessary for reasons of substantial public interest.

4. The reason why we collect this personal data

The Doctors, Nurses, Dentists and other Healthcare Professionals responsible for your care keep records about your health and any treatment and care you receive from DPHC. Your data are used to:
- Provide information to make health decisions made by care professionals with and for you;
- Make sure your care is safe and effective;
- Work with others providing you with care.

5. How else we may use your personal data

The personal data we collect about you may also be provided to other approved organisations, where there is a legal basis, to help with improving the care provided, research into new treatments and preventing illness. These help to provide better health and care for you, your family and future generations. Personal data about your health and care is only used in this way where allowed by law and would never be used for insurance or marketing purposes without your explicit consent.

You have a choice about whether you want your personal data to be used in this way, visit www.nhs.uk/my-data-choice. If you do choose to opt out, you can still consent to your personal data being used for specific purposes.

Where research identifies you as an individual we are required to meet our obligations under the common law rules on confidentiality and MOD will always ask for your consent to use your personal data before we do this. This will be explained to you prior to any research taking place.

Person identifiable data will only be used in research that has been independently reviewed and approved by an ethics committee.
In addition to the above we may also share your personal data with approved organisations to meet our obligations with the law. These may include:

• Looking after the health of the general public;
• Investigating concerns, complaints, claims or legal matters;

In some circumstances, we will anonymise your personal information so that it can no longer be associated with you, in which case we will use such personal data without further notice to you. Such instances may include:

• Preparing statistics on DPHC performance and activity
• Training and educating staff
• Audit and Statistics

6. Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal data for an unrelated or new purpose, we will notify you and we will explain the legal basis which allows us to do so.

7. Keeping your personal data safe and secure

Every member of staff who works for DPHC has a legal obligation to keep your personal data confidential. We maintain our duty of confidentiality by conducting annual training and awareness and ensuring access to personal data is limited to the appropriate staff. Personal data is only shared with organisations and individuals that have a legitimate and legal basis for access.

Our policy is to respect the privacy of our patients, their families and our staff and to maintain compliance with the common law duty of confidentiality, the GDPR, DPA18 and all UK-specific Data Protection Requirements.

We will only ever use or pass on your personal data if others involved in your care have a genuine need for it. Under the common law of confidentiality, we will not disclose your personal data to any third party without your permission unless there are exceptional circumstances (e.g where disclosure is necessary for the safety of someone), or where the law otherwise requires personal data to be passed on.

Our policy is to ensure all personal data related to our patients will be protected. All employees and sub-contractors who work with this practice are required to sign a confidentiality agreement.

The MOD has appointed Caldicott Guardians and Data Protection Advisors who are responsible for ensuring that the overall management of patient information and patient confidentiality is maintained.

8. How we store your personal data

Your personal data will be stored in secure government accredited Information Technology (IT) systems. We have put in place appropriate security measures to prevent your personal information from being accidentally lost, processed in an unauthorised way, altered or disclosed. Further information can be obtained from the SG Data Protection Advisor.

In some cases, we will process paper records and these will be managed and stored in accordance with our policies. Where possible, the physical information that is sent to your practice is transferred to the electronic patient record system.

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

We have put in place procedures to deal with any suspected data security breach and will notify you and the Information Commissioner's Office (ICO) of a suspected breach where we are legally required to do so.

9. Who we share your personal data with

Your personal data will only be shared if it is for the safe and effective provision of your care or required for our statutory function and legal obligations.
We may share your personal data with the following organisations:
• NHS Hospitals, Trusts/Foundation Trusts;
• Relevant GP Practices;
• Community services such as district nurses, rehabilitation services, telehealth and out of hospital services;
• Child health services that undertake routine treatment or health screening;
• Urgent care organisations, minor injury units or out of hours' services;
• Mental Health Trusts;
• Independent Contractors such as dentists, opticians, pharmacists;
• Private Sector Providers;
• Clinical Care Auditors;
• Clinical Commissioning Groups;
• Special Services and Law Enforcement Agencies;
• Those to whom you have asked us to provide your personal data;
• Other 'data processors' which you will be informed of;

We will, if necessary, transfer the personal data we collect about you to other departments outside the EU in order to perform our obligations or duties under the law.

10. How long we store your personal data

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. This is undertaken in accordance with our records management policy and procedures. After the retention period has elapsed, all personal data will be destroyed securely in line with MOD data destruction policy. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

11. Duty to inform

It is important that you tell the person treating you if any of your details have changed, such as your name or address, or if any of your details are incorrect, such as date of birth. Once informed we have an obligation to ensure your healthcare record is updated.

12. Your rights

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

• **Request access** to your personal data (commonly known as a "data subject access request" (SAR)). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

If you want to find out if MOD or any of our agencies hold any personal data about you, or want to make any corrections, you can make a 'subject access request' (SAR) under the GDPR. If we do hold personal data about you, we will:

- give you a description of it;
- tell you why we are holding it;
- tell you to whom it has or will be disclosed to; particularly if it has been disclosed to international organisations;
- let you have a copy of the personal data in a form that is as clear and understandable as possible.

Please be as specific as you can about the personal data you want.

You should be aware that some details in your health records may not be able to be given to you. This will be in the interests of your wellbeing or to protect the identity of a third party.

There are also a small number of cases where we do not have to give you the personal data you have asked for. For example, if we are using data for the purposes of investigating, preventing or detecting crime, or apprehending or prosecuting offenders where to do so would be likely to prejudice those purposes. In cases where it is known the police are investigating, or prosecuting offences, we will ask for their view on whether providing you with the personal data would prejudice their activities.

• **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected.

• **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data 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 data where you have exercised your right to object to processing.

• **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your situation which makes you want to object to processing on this ground.

• **Request the restriction of processing** of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.

• **Request the transfer of your personal data** allows you to obtain and reuse your personal data for your own purposes across different services.

There are some exceptions to the rights referred to above. Details of such restrictions will be provided to you if relevant.

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

• **Right to withdraw consent** - In the limited circumstances where you have provided your consent to the collection, processing and transfer of your personal data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time.

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

To comply with your request, we sometimes need to ask for specific information from you to help us confirm your identity and ensure your right to access the personal data (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

Further information can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

13. Objections / Complaints / Contacts

Should you have any concerns about how your personal data is managed at your DPHC practice please contact the Practice Manager or SG DPA. If you are still unhappy following a review, you have a right to lodge a complaint with the MOD Information Rights Team or Information Commissioner.

MOD Information Rights Team Ground floor, zone D Main Building Whitehall London SW1A 2HB **Email:** cio-dpa@mod.uk	Information Commissioner: Wycliffe house Water Lane Wilmslow Cheshire SK9 5AF Tel: 0303 123 1113 Email: casework@ico.org.uk https://ico.org.uk/global/contact-us/
SG Data Protection Advisor: Defence Medical Services (Whittington) Coltman House Lichfield Staffordshire WS14 9PY **Email:** SG-DPA@mod.gov.uk	The Ministry of Defence is the data controller. The contact detail is MOD Main Building, Whitehall, London SW1A 2HB **Email**: cio-dpa@mod.gov.uk

If you are happy for your data to be extracted and used for the purposes described in this privacy notice, then you do not need to do anything. If you have any concerns about how your data is shared or are dissatisfied with any aspect of this Privacy Notice, then please contact your Practice Manager or the SG DPA.

Changes: 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 will also notify you in other ways from time to time about the processing of your personal data.