Health Professionals Privacy Notice

We are committed to protecting your privacy when dealing with your personal information. This privacy notice provides details about the information we collect about you, how we use it and how we protect it. It also provides information about **your rights**.

If you have any questions about how we handle your information, please contact us at dataprotection@bupa.com.

This notice was last updated in March 2021.

1. Information about us

In this privacy notice, 'we', 'us' and 'our' mean The British United Provident Association Limited and its subsidiaries ('**Bupa**'). For company contact details, please visit:

www.bupa.co.uk/legal-notices/trading-addresses.

The Bupa company you are engaged by makes decisions about how your information is handled. (See below for an explanation of 'engagement'.)

2. What this privacy notice covers

This privacy notice applies to medical, dental and other health professionals who provide health services to our patients or customers but who are not directly employed by us ('**health professionals**'). In this document, we refer to this arrangement as an 'engagement'. We may give you further privacy information if necessary, for specific reasons.

3. How we collect personal information

We collect personal information from you and the people and organisations listed below.

We collect most of this personal information so that we can meet our obligations and we can manage our relationship with you properly. If you do not provide this personal information, these outcomes may not be possible.

We collect personal information from you if you provide this in the course of carrying out your role as a health professional to our patients or customers, or through your interactions with us generally, including by phone, by email, through our websites, on our portals or apps, by post, by filling in application or other forms, on social media or face-to-face (for example, in reviews, appraisals and so on).

We also collect personal information about you by monitoring your access to our premises (such as from CCTV, door entry systems and workplace health screening), your use of our devices and systems, and your use of any Bupa personal devices (if you use these for work).

Our *Acceptable Use Policy* (available here or by contacting us) provides more information about our monitoring activities, which we limit to make sure we do not invade your privacy.

We collect personal information from people and organisations such as:

- your agents (for example, legal representative, professional indemnity insurers);
- your referees and appraisers (for example, information we receive from your responsible officer ('**RO**') or clinical director);
- any service providers who work with us in relation to your engagement (for example, selection companies and providers of online assessments);
- doctors, other clinicians and health-care professionals, hospitals, clinics and other health-care providers, to help with workplace health and safety;
- your Bupa colleagues (for example, the other health professionals or Bupa employees you work with or those you report to);
- any Bupa customers or patients you provide treatment to or who you interact or work with in another way;
- our agents (for example, our legal representatives if we are involved in legal proceedings against you);
- credit-reference agencies, fraud-detection agencies, criminal-history reference agencies, if we need to carry out relevant checks (we will tell you at the time if we collect information from you to carry out these checks, and there is more information in the 'criminal offences information' section below);
- government departments (for example, the tax office or social security office);
- our regulators (for example, the Financial Conduct Authority, the Prudential Regulation Authority, data-protection supervisory authorities, and the Care Quality Commission) to make sure we are meeting the obligations we have by law;
- health regulators and registers that are relevant to your profession (for example, the General Medical Council ('**GMC**'), General Dental Council ('**GDC'**), Health and Care Professions Council, General Osteopathic Council, General Chiropractic Council, Nursing and Midwifery Council);
- sources which are available to the public, such as:
    - during your engagement, we may look at your LinkedIn page to get an overview of your professional history and qualifications, and we may also read any work you have had published that is relevant to the role we are considering you for, such as research or academic articles;
    - during your engagement, we may check the GMC's and GDC's websites to confirm your registration, whether you have any conditions of practise listed, and details of any hearings;
    - during your engagement, we may check your activity on publicly available social media networks, such as Facebook, Twitter and YouTube, if we have reason to suspect that you have broken our *Social Media Policy* (available here or by contacting us);
    - during your engagement, we may collect information from other third-party

organisations, including specialty-specific outcome measures from the clinical registries (such as the case-mix adjusted average number of years between the first revision and primary knee surgery by consultant, as reported by the National Joint Registry), as well as by the Private Healthcare Information Network ('**PHIN**');

- other Bupa companies, if a patient's treatment will be started by you and continued by another Bupa company (or vice versa) or if another Bupa company collects additional quality information, such as patient satisfaction surveys carried out by other Bupa companies; and
- after your engagement with us ends, we may look at your LinkedIn page to confirm that you are keeping to any restrictions in your contract.

4. Types of personal information

We process the following types of personal information about you.

- **Standard personal information** (for example, information we use to contact you, identify you or manage our relationship with you).
- **Special categories of information** (for example, health information in connection with medical leave, health information in connection with workplace health screening activities, information about your race, ethnic origin and religion for diversity and inclusion purposes).
- **Criminal offence information** about you (for example, information relating to criminal convictions and offences, or related security measures), in line with the terms of engagement which apply to you.

Standard personal information includes:

- contact information (for example, name, username, address, addresses for administration and practice locations, email address and phone numbers) for you and any contacts that are linked to you, such as your medical secretary or billing service;
- personal details (for example, the country you live in, your age, your date of birth and national identifiers such as your National Insurance number or passport number);
- information about your practise (for example, the date you were engaged by us, the date your engagement ended and the reasons for this (if this applies), the results of any reviews or appraisals, records of training, investigation and disciplinary matters);
- details of your previous work and your education, professional certificates and registrations, and other information from your CV;
- financial details (for example, bank details and how much we pay you (we share this information with HMRC for tax purposes));
- details of your professional indemnity insurance;
- professional references provided on your behalf;
- the results of any background checks (not including criminal-history checks) we have carried out on you in line with our local *Employment Screening Policies* and *Candidate's Guides to Bupa Employment Check Standards* (available here or by contacting us);
- photographs and videos from our CCTV systems;
- any information and images you provide for our (or a third party's) health professional directories;
- information related to you or your representative using our systems or portals; and
- the times you entered and left our offices (which we collect from our door entry systems).

Special category and criminal offence information includes:

- the results of any background checks (for example, by the Disclosure and Barring Service);

- information about your physical or mental health (this information may be included in sickness records, notes and reports about your health and any treatment and care you have received or need, and medical certificates, or information we collect during the course of workplace health screening (such as using thermal imaging or from checking your temperature); and
- information about your race, ethnic origin and religion (this information may be included in application forms, or you may choose to reveal it during your engagement to support diversity and inclusion initiatives).

5. What we use your personal information for

We process your personal information to:

- manage our relationship with you, our business and people and organisations who provide services for us;
- manage the cost of treatment provided to your patients who are our customers;
- protect our (or our customers' or other people's) rights, property or safety, including to maintain a safe working environment;
- exercise our rights, take legal action or defend ourselves from claims and to keep to laws and regulations that apply to us and the people and organisations we work with;
- take part in, or be the subject of, any sale, merger, outsourcing or takeover of all or part of the Bupa business; and
- consider and act upon whistleblowing reports we receive, as set out in our local *Speak Up Policies* (available here or by contacting us).

6. Legal grounds

By law, we must have a lawful reason for processing your personal information. These are set out below.

Standard personal information: We process standard personal information about you if:

- it is necessary to meet the obligations set out in a contract with you or to take steps which you have asked us to take before entering into a contract – if we have a contract with you, we will process your personal information to fulfil that contract (for example, to pay you for your service or services);
- it is in our own or a third party's legitimate interests (see below for more details); or
- we have to or are allowed to do so by law.

Special category information: We process special category information about you if:

- it is necessary in the vital interests of you or another person (for example, if you need medical attention at work and are unable to communicate or give your consent);
- you have obviously made that personal information public (for example, you publicly share sensitive personal information on the intranet);
- it is in the public interest, in line with local laws;
- it is necessary to establish, make or defend legal claims; and
- it is necessary for the purposes of occupational medicine, including to assess whether you are able to work.

Criminal offences information

When you work with us, we make sure you are fit and proper to fulfil your role. By doing this we are protecting our patients, residents, employees, business reputation and assets. This will mean that we will carry out a criminal history check, at a level that is appropriate to you and in line with the services you provide to our customers or your terms of engagement with us.

7. Legitimate interest

We process your personal information for a number of legitimate interests. Taking into account your interests, rights and freedoms, the types of legitimate interest which allow us to process your personal information include:

- to find the best talent and make sure you are ready to deliver your services at Bupa;
- to build the capability of health professionals to help our organisation grow, now and in the future;
- to make sure that health services provided to our customers are high quality and that the cost of those services is reasonable;
- to reward health professionals in a way that attracts and helps us keep the best in the market;
- to provide health professionals and their teams (for example medical secretaries) with support on a full range of day-to-day matters, and to otherwise manage our relationship with you, our business and people and organisations who provide services on our behalf;
- to make sure we are set up for success and to deliver our strategic vision through strategic resource planning;
- for statistical research and analysis so that we can monitor and improve products, services, websites and apps, or develop new ones;
- to protect our (or our customers' or other people's) rights, property or safety including to protect the health, safety and welfare of workers and health professionals, and to maintain a safe working environment;
- to tell other organisations you work for if we have serious concerns about patient safety or if you have not met the relevant clinical standards during your engagement with us;
- to monitor how well we are meeting our clinical and non-clinical performance expectations;
- to exercise our rights, to respond to complaints, to take legal action or defend ourselves from claims and to keep to laws and regulations that apply to us and the people and organisations we work with; and
- to take part in, or be the subject of, any sale, merger, outsourcing or takeover of all or parts of the Bupa business or for us to take over another business.

8. Sharing your information

We share your information, for the purposes set out in this privacy notice, with:

- other members of the Bupa Group;
- our customers, or potential customers;
- other organisations you belong to, or are professionally associated with;
- other organisations you work for if we have serious concerns about patient safety or if you have not met the relevant clinical standards during your engagement with us;
- users of our health professional directories that are available to the public;
- doctors, clinicians and other health professionals, hospitals, clinics and other health providers and medical assistance providers;
- our insurers;
- our agents (for example, our legal representatives, translators, interpreters and tax advisers in line with the law);
- suppliers who help deliver products or services on our behalf;
- any corporate clients you provide services to on-site, if your role involves this;
- people or organisations we have to, or are allowed to, share your personal information with by law (for example, for safeguarding purposes);

- the police and other law-enforcement agencies to help them perform their duties, or with others if we have to do this by law or under a court order;
- government authorities, agencies and other regulators including the Care Quality Commission who may access care records and other personal information as part of their regulatory activity (their privacy notice is available at www.cqc.org.uk/about-us/our-policies/privacy-statement), the Financial Conduct Authority, the Prudential Regulation Authority, data-protection supervisory authorities, the Health Protection Agency, PHIN, the GMC and the GDC;
- other regulators, including the Medicines and Healthcare products Regulatory Authority (which makes sure that medicines and medical devices used in the UK work and are safe), the Human Fertilisation and Embryology Authority (which regulates and inspects all of our clinics which provide fertility services or which store eggs, sperm or embryos), NHS England (which leads the NHS in England) and the Department of Health (the government department responsible for health and adult social care policy);
- other third parties we work with to provide our products and services, such as other insurers and reinsurers, actuaries, auditors, solicitors, debt-collection agencies, credit-reference agencies, fraud-detection agencies (including health-insurance counter-fraud groups);
- if any member of the Bupa group of companies sells or buys any business or assets, the potential buyer or seller of that business or those assets; and
- a third party who takes over any or all of the Bupa group of companies' assets.

If we share your personal information, we will make sure appropriate protection is in place in line with data-protection laws.

9. Transferring information outside the UK and the European Economic Area (EEA)

We deal with many international organisations and use global information systems. As a result, we may transfer your personal information to other countries for the purposes set out in this privacy notice. This may include transferring information from within the UK to outside the UK, and from within the EEA (the EU member states plus Norway, Liechtenstein and Iceland) to outside the EEA for example to Australia.

We take steps to make sure that, when we transfer your personal information to another country, appropriate protection is in place in line with data-protection laws. Often, this protection is set out under a contract with the organisation who receives that information. For more information about this protection, please contact us at dataprotection@bupa.com.

10. How long we keep your personal information

We keep your personal information in line with set periods. We use the following criteria to help us decide how long we need to keep your personal information for.

- Whether you are currently engaged by us.
- How long it is reasonable to keep records to show we have met the obligations we have to you, to our customers and the patients you have treated, and the obligations we have by law.
- Any periods for keeping information which are set by law or recommended by regulators, professional bodies or associations.
- Any time limits for making a claim.
- Any tribunal, court or other relevant proceedings that apply.
- How long it would be reasonable to expect you to ask for a reference.
- Whether or not we have an ongoing commercial relationship with you.

At the end of the period worked out using the above criteria, we will securely and permanently delete the personal information in your file. If you would like more information about how long we will keep your information for, please contact us at dataprotection@bupa.com.

We are committed to keeping your information secure, and will store it in line with our *Enterprise*

Security Policy (available here or by contacting us).

11. Your rights

Under data-protection laws in the UK and EEA, you have the following rights relating to the information we hold about you in some computer and paper records.

- **Right of access:** You have the right to make a written request for details of the personal information we hold about you and a copy of that personal information.
- **Right to rectification:** You have the right to have inaccurate information about you corrected.
- **Right to erasure ('right to be forgotten'):** You have the right to have certain personal information about you deleted from our records.
- **Right to restriction of processing:** You may have the right to ask us to use your personal information for restricted purposes only.
- **Right to object:** You have the right to object to us using your personal information in certain circumstances.
- **Right to data portability:** You have the right to ask us to transfer personal information you have given us to you or someone else in a format that can be read by computer.
- **Right to withdraw consent:** We do not normally rely on your permission to process your personal information. We will only ask for your permission in very limited circumstances and, if we do so, we will make it obvious to you when we are asking for permission and what it is for. You have the right to withdraw any permission you have given us to handle your personal information. If you withdraw your permission, this will not affect the lawfulness of how we used your personal information before you withdrew your permission.

These rights may not apply in all cases. If we are not able to meet your request, we will explain why.

If you make a request, we will ask you to confirm your identity if we need to, and to provide information that helps us to understand your request better.

If you would like more information about your rights, or to exercise any of your rights, please contact us at dataprotection@bupa.com.

12. Data-protection contacts

If you have any questions, comments, complaints or suggestions relating to this notice, or any other concerns about the way in which we process information about you, please contact our Data Protection Officer and Privacy Team at dataprotection@bupa.com.

You also have a right to make a complaint to your local data-protection supervisory authority. Our main office is in the UK, where the local supervisory authority is the Information Commissioner.

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

Phone: 0303 123 1113 (local rate) or 01625 545 745 (national rate).

In Ireland, the local supervisory authority is the Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2, D02 RD28, Ireland.

Email: info@dataprotection.ie

You can also make a complaint to the supervisory authority which is based in the country or territory where:

- you live;

- you work; or
- the matter you are complaining about took place.