



Privacy Policy

Healthcare Providers

This Privacy Policy tells you what data we collect, why we collect it and what we do with it. You can also find information on the controls you have to manage your data within these pages.

Entity AXA PPP healthcare Ltd
Date April, 2021

Contents

1. Our Privacy Principles	2
2. How do we collect your personal information?	3
3. What personal information do we collect?	4
4. How do we use your personal information?	4
5. Who do we share your personal information with?	10
6. How long do we keep records for?	12
7. Your Rights	12
8. Marketing	14
9. Contact Details of the Data Protection Officer	15
10. Contact Details for AXA	16
11. AXA's data privacy declaration	16



AXA Health companies are all committed to ensuring personal information is protected. Any document that referred you to this notice set out details of the AXA company that is processing your personal information; it is the data controller of your personal information and is responsible for complying with data protection laws. If you came straight to this document from our website the data controller is AXA PPP healthcare Ltd. For the purposes of this Privacy Policy, references to "**we**" or "**us**" shall refer to that AXA company.

Where you have provided information to us about a third party who has consented to you doing so on their behalf, this Privacy Policy should be brought to their attention.

By providing your personal information to us or on behalf of another party, you acknowledge that we may use it in the ways set out in this Privacy Policy. We may provide you with further notices highlighting certain uses we wish to make of your personal information.

From time to time we may need to make changes to this privacy policy, for example, as the result of government regulation, new technologies, or other developments in data protection laws or privacy generally. You should check the healthcare provider section of the AXA Health website periodically to view the most up to date privacy policy.

1. Our Privacy Principles

When we collect and use your personal information, we ensure we look after it properly and use it in accordance with our privacy principles set out below, keep it safe and will never sell it.

1. Personal information you provide is processed fairly, lawfully and in a transparent manner
2. Personal information you provide is collected for a specific purpose and is not processed in a way which is incompatible with the purpose which AXA collected it
3. Your personal information is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
4. Your personal information is kept accurate and, where necessary kept up to date
5. Your personal information is kept no longer than is necessary for the purposes for which the personal information is processed
6. We will take appropriate steps to keep your personal information secure
7. Your personal information is processed in accordance with your rights
8. We will only transfer your personal information to another country or an international organisation outside the European Economic Area where we have taken the required steps to ensure that your personal information is protected. Such steps may include placing the party we are transferring information to under contractual obligations to protect it to adequate standards



9. AXA UK and AXA Group companies do not sell your personal information and we also do not permit the selling of customer data by any companies who provide a service to us
10. We endeavour to be transparent and clear with the way we use your personal information

2. How do we collect your personal information?

Whilst there are a number of ways in which we collect your personal information, the two main ways we might collect personal information about you are from things you tell us yourself, and from things other people or organisations share with us. Things you tell us could include conversations we have on the phone, what you've written on a registration form or information in an invoice. We might also collect information about you from other people and organisations, such as medical facilities and regulatory bodies, or by checking databases, such as the electoral register. Please see below for a more detailed list of ways we collect your personal information:

We collect personal information directly from you:

- via enquiry and registration forms;
- via feedback forms and forums;
- when you fill out a survey, or vote in a poll on our website;
- via cookies. You can find out more about this in our cookies policy <https://www.axahealth.co.uk/cookie-policy/>
- via our telephone calls with you, which may be recorded;
- when you provide your details to us either online or offline;
- via our partner Healthcode for registration and billing purposes

We also collect your personal information from a number of different sources including:

- from social media and other publicly available sources when fraud is suspected; and
- via third parties including:
 - medical professionals and hospitals;
 - Medical billing agencies you have enlisted to manage your invoicing and payment
 - Regulatory bodies such as General Medical Council (GMC)
 - Medical secretaries



3. What personal information do we collect?

We might collect personal information, such as your contact details or information about your bank account. The information we collect depends on our relationship with you; for example if you have admitting rights to a number of hospitals we may collect this data or if you practice from various locations we may collect the addresses of these locations. Please note, in certain circumstances we may request and/or receive "sensitive" personal information about you. For example, details of any court or HMRC judgments for the purposes of preventing, detecting and investigating fraud. Please see below for a more detailed list of personal information we collect.

Where you have requested a named contact to discuss details on your behalf we may ask you for details of this third party.

We may collect the following information about you:

- Personal information
 - contact details such as name, email address, postal address and telephone number
 - named 3rd parties on your registration such as medical secretary or a billing agency you have tasked to manage your accounts.
 - identification information such as your GMC number, area of speciality and facilities where you have admitting rights.
 - financial information such as bank and billing details
 - information obtained through our use of cookies. You can find out more about this in our cookies policy <https://www.axahealth.co.uk/cookie-policy/>
 - information relevant to your involvement in a matter giving rise to a claim
 - your marketing preferences

- Sensitive personal information
 - details regarding criminal offences, including alleged offences, criminal proceedings, outcomes and sentences

4. How do we use your personal information?

We mainly use your personal information to maintain a professional relationship with you and to support our members when making a claim. We will use your personal information to ensure you are reimbursed for the treatment and services you provide to our members, in line with their policy rulings and our terms. However, there are a number of other reasons why we use your personal information; please see below for a more detailed list.

Under data protection laws we need a reason to use and process your personal information and this is called a legal ground. We have set out below the main reasons why we process your personal information and the applicable circumstances when we will do so. When the



personal information we process about you is classed as sensitive personal information (such as details about your health or criminal offences) we must have an additional legal ground for such processing.

- Where we have a legal or regulatory obligation to use such personal information, for example, when our regulators, the Prudential Regulatory Authority, (PRA), the Financial Conduct Authority (FCA) and our data protection regulator, the Information Commissioner's Office (ICO) wish us to maintain certain records of any dealings with you.
- Where we need to use your personal information to establish, exercise or defend our legal rights, for example when we are faced with any legal claims or where we want to pursue any legal claims ourselves.
- Where we need to use your personal information for reasons of substantial public interest, such as investigating fraudulent claims, malpractice, improper conduct incompetence, unfitness and carrying out fraud, credit, international sanctions and anti-money laundering checks.
- Where you have provided your consent to our use of your personal information - We will usually only ask for your consent in relation to providing marketing information to you (including information about services). If we need it elsewhere this will be made clear when you provide your personal information. If we ask for your consent we will explain why it is necessary. Without your consent in these circumstances, we may not be able to fulfil the terms of our agreement with you. Where you provide sensitive personal information about a third party (such as a patient) we may ask you to confirm that the third party has provided his or her consent.
- Where we or others have appropriate legitimate need to use your personal information such as maintaining our business records, reviewing your billing or healthcare practices, arranging for members' diagnostic test results to be sent to you, letting healthcare facilities and customers know which healthcare providers we work with, developing and improving our products and services, all whilst ensuring that such need does not interfere with your rights and freedoms.



You will find details of the legal grounds we rely on for each use of your personal information below.

Why we need your personal information	Personal information we may process for the purpose adjacent shall include but shall not be limited to the types of information set out below	Legal Grounds for Processing
To communicate with you and resolve any complaints you may have and undertaking experience and satisfaction surveys	Your contact details and any information relevant to your agreement or relationship with AXA Health.	Legal grounds: we have a legitimate business need to resolve any complaints and to find out how you view your relationship with us and the services we offer. Legal grounds for sensitive personal information: such use is necessary for the purposes of establishing, exercising or defending our legal rights and/or you have provided your consent. To protect the public against dishonesty, malpractice, improper conduct, unfitness or incompetence
To evaluate your application to become a recognised specialist or practitioner with AXA Health and manage our relationship.	Your contact details, confirmation of medical indemnity insurance, other personal details such as regulatory body registration numbers and your areas of expertise and specialism and bank account details	Legal ground: such use is necessary in order to take steps to enter an agreement with you and fulfil our obligations as part of this agreement.



<p>To support our customers by identifying and informing them of appropriate healthcare providers to treat them, arranging appointments etc.</p>	<p>Your contact details, your areas of expertise and specialism, your practicing locations and admitting rights</p>	<p>Legal grounds: it is in the legitimate interest of ourselves, our customers and you for us to inform our customers about your services and make arrangements for them to see you.</p>
<p>To prevent, detect and investigate fraud, dishonesty, malpractice, improper conduct, unfitness or incompetence. More information on how we use your information do this is available under Detail Section 6 below.</p>	<p>Information about you, your name, address, email address and contact details.</p> <p>Information about your speciality, practicing locations and admitting rights.</p>	<p>Legal grounds: such use is necessary in order to fulfil our obligations once becoming a recognised specialist or practitioner and there is a public interest to prevent fraud, dishonesty, malpractice, improper conduct, unfitness or incompetence.</p> <p>Legal ground for sensitive personal information: for reasons of substantial public interest to prevent and detect fraud, dishonesty, malpractice, improper conduct, unfitness or incompetence.</p>
<p>For the purposes of payment of invoices for treatment and debt recovery (where you have been overpaid for treatments provided or have billed outside of the terms in any agreement that maybe in place).</p>	<p>Information about you, your name, address, email address, contact details and bank account details</p>	<p>Legal ground: to enable to performance of a contract or agreement in place</p>



<p>For our own management information purposes; including managing our business operations such as maintaining accounting records, analysis of financial results, internal audit requirements, receiving professional advice (e.g. tax or legal advice). We also undertake measures to secure our system and to ensure the effective operation of our systems. More information on how we use your information is available under Detail Section 3 below.</p>	<p>Information about you, your name, address, email address and contact details.</p> <p>Information about your working practices such as treatments carried out, payment values and frequencies.</p>	<p>and maintain appropriate records, to protect the security of our systems</p> <p>Legal ground for sensitive personal information: for reasons of substantial public interest to prevent and detect fraud, dishonesty, malpractice, improper conduct, unfitness or incompetence.</p>
<p>For analytical purposes and to improve our products and services. More information on how we use your information do this is available under Detail Section 4 below.</p>	<p>Information about you, your name, address, email address and contact details.</p> <p>Information about your working practices such as treatments carried out, payment values and frequencies.</p>	<p>Legal ground: we have a legitimate business need to use your personal information for services improvement.</p>
<p>Complying with our legal or regulatory obligations such as conducting money laundering checks or responding to demands for information from public authorities</p>	<p>Details about you, contracts or agreements in place, financial information or registration with relevant regulatory body depending on the nature of the obligation</p>	<p>Legal ground: such use is necessary for us to comply with our legal or regulatory obligations</p>
<p>Providing improved quality, training and security (for example, with respect to recorded or monitored phone calls to our contact numbers)</p>	<p>Details about you and other related parties, treatment you have carried out or payment enquiries following discussion with you or your representative during a telephone conversation with us.</p>	<p>Legal ground: such use is necessary for us to comply with our legal or regulatory obligations</p>



Providing marketing information to you (including information about other services relating to our relationship with you) in accordance with preferences you have expressed.	Your name, contact details, marketing preference	Legal ground: we have your consent
To let healthcare facilities know which healthcare providers we particularly work with to help them manage their relationship with you.	Information about you, your name and contact details.	Legal ground: is necessary in the legitimate interest of our customers to help improve choice and access to healthcare and of healthcare facilities to further their relationship with you.
To facilitate your receipt of diagnostic test results (including scans) for patients that we direct to you, where those tests were ordered by a third party, such as our Dr@Hand service.	Information about you, your name, address, email address and contact details.	Legal ground: such use is necessary in the legitimate interests of your patient.

Detail Section 3 – How does AXA Health use your information for Management Information purposes?

We use your personal information to help us understand our business, the wider healthcare environment and to monitor our performance, for example, to help determine the demand for a particular speciality by geographical area.

Detail Section 4 – How does AXA Health use your information for analytical purposes and to improve our products and services?

We may use your personal information for research and statistical analysis including general research into health-related areas and research about the products and services we provide. By analysing information provided we can tailor-make and improve our products to better suit our customer's needs.

Where possible, we will anonymise such information. However, sometimes we may need to use your personal information to do this and where we do we will obtain your consent beforehand if necessary.



Detail Section 6 – How does AXA Health use your personal information to prevent, detect and investigate fraud, malpractice etc.?

To help keep premiums and costs down we work with other insurers, healthcare providers including the NHS, anti-fraud bodies and law enforcement agencies to protect ourselves, the NHS and our policyholders from fraudulent behaviour and medical malpractice. This may mean disclosing personal information to these bodies. In some cases, we provide your personal information to insurance fraud databases, which are accessible by some or all of these bodies. We are obliged to report suspicions of medical malpractice to the relevant regulatory body such as the General Medical Council and we have a Memorandum of Understanding regarding data sharing in place with the Care Quality Commission.

We also monitor the services being provided by healthcare providers for these purposes and to ensure accurate billing. In some cases, we are required by law to report crime and suspected crime and other matters to law enforcement and government agencies.

5. Who do we share your personal information with?

We might share your personal information with companies inside the AXA Group, and other third parties outside the Group. For further details of all disclosures, please see below. We won't share any of your personal information other than for the purposes described in this Privacy Policy.



Who might we disclose your personal information to?

Disclosures within our group

In order to provide our services your personal information is shared with other companies in the AXA Group including, but not limited to AXA PPP healthcare Administration Services Limited. Your personal information might be shared for our general business administration purposes.

Disclosures to third parties

We also disclose your information to the third parties listed below for the purposes described in this Privacy Policy. This might include:

- Your current patients (this may include your account/billing address and bank details so that your patients can pay you any amounts that they are liable for) and potential patients
- Your medical secretary or your lawyer
- Third party service providers we both use such as Healthcode
- Hospitals and other healthcare facilities to let them know which healthcare providers we work with
- Other healthcare service providers to support your patients' care.
- Our third party services providers such as IT suppliers, actuaries, auditors, lawyers, marketing agencies, document management providers and tax advisers
- Financial organisations and advisers
- Central and local Government (for example if they are investigating fraud or because we need to contact them regarding international sanctions)
- The Financial Ombudsman Service and regulatory authorities such as the Financial Conduct Authority, the Care Quality Commission and the Information Commissioner's Office
- Other insurance companies, NHS fraud teams, the General Medical Council, the police, National crime agency, other law enforcement agencies and organisations that maintain anti-fraud or other crime databases where reasonably necessary for the prevention or detection of crime
- Selected third parties in connection with the sale, transfer or disposal of our business

We may also disclose your personal information to other third parties where:

- We are required or permitted to do so by law or by regulatory bodies such as where there is a court order, statutory obligation or Prudential Regulatory Authority / Financial Conduct Authority or Information Commissioners Office request; or
- We are required to do so following a request from Financial Ombudsman Service as a result of an escalated complaint.



- We believe that such disclosure is necessary in order to assist in the prevention or detection of any criminal action (including fraud) or is otherwise in the overriding public interest.

Some of the recipients set out above may be in countries outside of the UK and EEA notably in i) Switzerland, where AXA has a European Data Centre, and ii) India, where some administration is undertaken. Where we make a transfer of your personal information outside of the EEA we will take the required steps to ensure that your personal information is protected. Such steps may include placing the party we are transferring information to under contractual obligations to protect it to adequate standards. Occasionally there may also be some circumstances where we are required to transfer your personal information outside of the EEA and we shall rely on the basis of processing it for being 'necessary for the performance of your contract.

6. How long do we keep records for?

In most cases, we only keep your information for as long as the regulations say we have to or for as long as we need to be able to establish facts in the event of query or legal action. This is usually between three and ten years after our relationship with you ends but it will vary depending on what data we hold, why we hold it and what we're obliged to do by the regulator or the law.

How long do we keep records for?

We will only keep your personal information for as long as reasonably necessary to fulfil the relevant purposes set out in this Privacy Policy and in order to comply with our legal and regulatory obligations. The time period we retain your personal information for will differ depending on the nature of the personal information and what we do with it. How long we keep personal information is primarily determined by our regulatory obligations. We typically keep records for up to 10 years from the end of our relationship with you. In some cases, such as if there is a dispute or a legal action we may be required to keep personal information for longer.

7. Your Rights

You can ask us to do various things with your personal information. For example, at any time you can ask us for a copy of your personal information, ask us to correct mistakes, change the way we use your information, or even delete it. We'll either do what you've asked, or explain why we can't - usually because of a legal or regulatory issue.

For further details about your rights please see below.

You have the following rights in relation to our use of your personal information:



The right to access your personal information

You are entitled to a copy of the personal information we hold about you and certain details of how we use it. There will not usually be a charge for dealing with these requests. Your personal information will usually be provided to you in writing, unless otherwise requested, or where you have made the request by electronic means, in which case the information will be provided to you by electronic means where possible.

The right to rectification

We take reasonable steps to ensure that the personal information we hold about you is accurate and complete. However, if you do not believe this is the case, please contact us here and you can ask us to update or amend it.

The right to erasure:

In certain circumstances, you have the right to ask us to erase your personal information, for example where the personal information we collected is no longer necessary for the original purpose or where you withdraw your consent. However this will need to be balanced against other factors, for example according to the type of personal information we hold about you and why we have collected it, there may be some legal and regulatory obligations which mean we cannot comply with your request. Please note that if you withdraw your consent we may not be able to process payments or review historical payments for treatment carried out on our members.

Right to restriction of processing:

In certain circumstances, you are entitled to ask us to stop using your personal information, for example where you think that the personal information we hold about you may be inaccurate or where you think that we no longer need to process your personal information.

Right to data portability:

In certain circumstances, you have the right to ask that we transfer any personal information that you have provided to us to another third party of your choice. Once transferred, the other party will be responsible for looking after your personal information.

Right to object to direct marketing:

You can ask us to stop sending you marketing messages at any time. Please see section 8 for more information.



Right not to be subject to automated-decision making:

Some of our decisions are made automatically by inputting your personal information into a system or computer and the decision is calculated using certain automatic processes rather than our employees making those decisions. We make automated decisions in the following situations:

The right to withdraw consent:

For certain uses of your personal information, we may ask for your consent. Where we do this, you have the right to withdraw your consent to further use of your personal information. Please note in some cases we may not be able to process your payments for treatment carried out on our members if you withdraw your consent.

The right to lodge a complaint

You have a right to complain to the ICO at any time if you object to the way in which we use your personal information. More information can be found on the Information Commissioner's Office website: <https://ico.org.uk/>

You can make any of the requests set out above using the contact details provided to you in your registration pack or alternatively, as set out in section 11. Please note that in some cases we may not be able to comply with your request for reasons such as our own obligations to comply with other legal or regulatory requirements. However, we will always respond to any request you make and if we can't comply with your request, we will tell you why.

In some circumstances exercising some of these rights (including the right to erasure, the right to restriction of processing and the right to withdraw consent) may mean we are unable to maintain our relationship with you; resulting in the lapse of your recognition as registered healthcare professional with us.

8. Marketing

You're in control of how we use your information for marketing. We will only contact you if you've agreed it's okay. Then, we might use your information to tell you about services, arrangements or opportunities that could interest you. But we don't use your personal information for our online ad campaigns – you'll need to check your browser or social media settings to avoid seeing these.

We are committed to only sending you marketing communications that you have clearly expressed an interest in receiving. If you wish to unsubscribe from emails sent by us, you



may do so at any time by clicking on the "unsubscribe" link that appears in all emails. Otherwise you can always contact us using the details set out in section 11 to update your contact preferences. In such circumstances, we will continue to send you service related (non-marketing) communications where necessary.

We would like to keep you informed, from time to time about relevant services. We may do this by mail, email, telephone or other electronic methods such as text message.

From time to time we may run specific marketing campaigns through social media and digital advertising that you may see which are based on general demographics and interests. Individual personal information is not used for these campaigns. If you do not want to see any campaigns then you will need to adjust your preferences within social media settings and your cookie browser settings.

9. Contact Details of the Data Protection Officer

If you wish to contact the Data Protection Officer the details are below:

For AXA Health

The Data Protection Officer:

AXA Health
Jubilee House
Vale Road,
Tunbridge Wells
Kent
TN1 1BJ

email address: Data.Protection@axa-health.co.uk

If you do not wish to deal direct with AXA Health then you can contact our head office:

The Data Protection Officer:

AXA UK Plc
20 Gracechurch Street
London EC3V 0BG

email address: ukgroupprivacy@axa-uk.co.uk

If you would like to contact the UK's Information Commissioner's Officer direct; please write to the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, Telephone: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number <https://ico.org.uk/global/contact-us/email/>



10. Contact Details for AXA

AXA Group

Wherever the name “AXA” is used on the Website, this implies one or more of the following companies within the AXA Group of companies, which may offer products or services on the Website. Further details can be found on the respective companies’ websites.

AXA Health Limited AXA Health Limited

Trading as AXA Health, a private limited company incorporated in England and Wales with company number 12839134 and whose registered office is at 20 Gracechurch Street, London EC3V 0BG

AXA PPP healthcare Limited

Trading as AXA Health, a private limited company incorporated in England and Wales with company number 03148119 and whose registered office is at 20 Gracechurch Street, London EC3V 0BG

AXA PPP healthcare Administration Services Limited

Trading as AXA Health, a private limited company incorporated in England and Wales with company number 03429917 and whose registered office is at 20 Gracechurch Street, London EC3V 0BG

AXA UK plc

Registered Company Number: 02937724

Registered Office: 20 Gracechurch Street, London EC3V 0BG

11. AXA’s data privacy declaration

Your personal information can help us give you a better, more personalised service. But looking after that data is a big responsibility. We take our responsibilities seriously, so we’ve introduced internationally-recognised data privacy rules to protect you. We keep your data safe, confidential and will never sell it. And, if you ask us to, we’ll tell you exactly what information we have so you can be sure it’s up-to-date and accurate.

AXA’s Data Privacy Declaration

AXA's mission is to help you, our customers, live your lives with more peace of mind by protecting your family, your property and your assets against risks. Doing so involves the



collection of data so that we understand the nature of these risks that we cover for you, and that we may provide you with the right products and services to meet your needs.

Today's world is one in which the amount of available data is growing exponentially. Ultimately, this allows us to enhance your experience through tailor-made protection, more relevant information and simplified, efficient procedures.

We believe that protecting your personal information is essential when seizing these opportunities. This is why we considered it important to share with you the principles that will guide us with regard to the treatment of personal information.

11.1. Our Commitment to Safeguard Personal information

We know that respecting the confidentiality of personal information is critical to preserving your trust and therefore have developed security procedures and we use a range of organisational and technical security measures designed to protect your personal information from unauthorized use or disclosure.

We have a Data Privacy team at a global level and a network of Data Privacy Officers throughout our businesses to oversee data safety.

We are the first insurance group to have adopted Binding Corporate Rules. These rules represent an internationally recognized standard for protection of personal information and are an adequate safeguard for transferring your personal information to our group companies outside the European Economic Area. They were approved by the French Data Protection Authority (CNIL) and 15 other EU Data Protection Authorities including the UK's Information Commissioner's Office.

11.2. Our Commitment with Respect to the Use of Personal information

We provide you with up-to-date prevention and protection solutions, through an in-depth and well-informed understanding of the risks you face. To do this, we collect your personal information and use it in compliance with data protection laws.

We have in place procedures and contractual arrangements designed to ensure that all employees, sales representatives, advisers and service providers keep client files confidential.

Our customers often entrust us with sensitive personal information in connection with insurance coverage we provide to them - both at the time of their initial subscription and during the term of their coverage. We view ourselves as custodians of this data and do not sell it to third parties outside the AXA Group. We may market products jointly with other



companies in cases where we believe there is a unique or compelling value proposition for our customers.

11.3. Our Commitment to Dialogue and Transparency

As a leading international insurance group, we play a proactive role in public policy and regulatory debates around personal information protection.

These are our continuing commitments to you. We will keep pace with future developments surrounding data privacy to adapt them to your evolving needs.

> For more information, please feel free to contact privacy@axa.com