

Employee Privacy Notice

Effective 9 June 2025

Oxehealth Limited and/or its subsidiaries ("Oxehealth", "we", "us", or the "Company") are responsible for the processing of your Personal Data as described in this Privacy Notice, unless specified otherwise. As the controller of your Personal Data, we determine how and why your data is processed and ensure that all processing activities comply with applicable legal requirements.

At Oxehealth, we respect your privacy and we want to be as transparent as possible about how we collect, use, and protect your data, including Personal Data. For the purposes of this Privacy Notice, "Personal Data" means any information that relates to an identified or identifiable individual and includes what may be referred to as "Personal Information" under applicable US privacy laws.

As a Data Controller we are committed to complying with the relevant data protection laws in the jurisdictions where we operate. This includes but is not limited to the EU and UK General Data Protection Regulations and the California Consumer Privacy Act (as amended by the California Privacy Rights Act).

This Privacy Notice applies specifically to current and past job applicants and employees (including permanent staff, interns, contract staff and advisors on the Oxehealth payroll) and sets out the way in which we process, protect, and manage your Personal Data. This includes data provided directly by you or collected from others during your application process, employment or post-employment period with Oxehealth.

In this notice we will explain who we are, who our Data Protection Officer is, how we collect your information, what information we collect about you and what we use it for, our lawful basis for processing your personal data, how we store and keep your information secure, how long we keep your information for, who your information is shared with, and transfers to third countries. This notice also explains your data rights, including your rights to access, correct, or restrict our use of your personal data, how to contact us about these rights, and how to contact us and the supervisory authorities in the event you have a complaint.

1. Who we are

Oxehealth, We, Us, Our refers to the following group of companies:

Holding company and main office (UK)

Oxehealth Limited

Registered in England and Wales, Company Registration Number 08163325

Address: Bee House, Eastern Avenue, Milton Park, Abingdon, England, OX14 4SB

Fully owned subsidiaries:

Oxehealth Inc

Registered in the United States of America, No. 3389479

Address: 9419 North Market Street, Suite 950 Wilmington, 19801 Delaware

Oxehealth AB

Registered in Sweden, Registration Number 559275-7487

Address: Nordenskiöldsgatan 11, 21119 Malmö

2. What Personal Data we may collect about you, what we use it for, where we collect it from and our legal basis for processing

Job Applications:

To assess your suitability for an internship or job at Oxehealth for a role you have applied for or other potentially suitable roles, to communicate with you about your application for a role with us, and to request references relating to your application we may collect and use the following information:

What Personal Data we collect and use	Where we collect your Personal Data from
<ul style="list-style-type: none">• Name• Address• Personal Email and Telephone contact information• Social Media Handles• CV Information (including education and job history)• Interview Notes• Interview Test• Interview Outcomes• Reference details• Offer details	<ul style="list-style-type: none">• Directly from you• Social Media and Job sites such as Indeed, Linked-In• Recruitment Agencies• Employer or academic institution• Reference contacts provided by you.

Oxehealth has a legitimate interest to process job applications for vacancies, inform applicants of their application outcome and offer a position to a suitable candidate.

Employment Contracts:

To enter into a contract of employment with you we may collect and use the following information:

What Personal Data we collect and use	Where we collect your Personal Data from
<ul style="list-style-type: none">• Name• Home Address• Personal Email and Telephone contact information	<ul style="list-style-type: none">• Directly from you

Oxehealth enters into contracts with employees to fulfil its legal obligations under the Employment Rights Act 1996.

Right to work and Security Screening:

To carry out right to work checks and baseline personnel security screening checks we may collect and use the following information:

What Personal Data we collect and use	Where we collect your Personal Data from
<ul style="list-style-type: none"> • Employment history • Address history • Recent bills • Passport copy • Driving License • Birth Certificate • NI Number • Employment gaps • Criminal record • Name • Work Email Address 	<ul style="list-style-type: none"> • Directly from you • Security Clearance Providers

Oxehealth has a legitimate interest to carry out screening to ensure compliance with customer contractual obligations and comply with Oxehealth's security and privacy policies and a legal obligation to carry out right to work checks in compliance with the Immigration, Asylum and Nationality Act 2006.

Providing equipment and access to business services:

To provide you with equipment, IT onboarding and access to business services required to do your role, and to collect equipment from you at the end of your employment we may collect and use the following information:

What Personal Data we collect and use	Where we collect your Personal Data from
<ul style="list-style-type: none"> • Name • Home Address • Personal Email and Telephone contact information • Employment start and end dates. 	<ul style="list-style-type: none"> • Directly from you • From your line manager

Oxehealth has a legitimate interest in managing Oxehealth equipment and business services.

Processing Payroll and Providing Benefits:

To process payroll, provide your pension, and manage sick leave, maternity / paternity leave and other employee benefits agreed in your contract with you we may collect and use the following information:

What Personal Data we collect and use	Where we collect your Personal Data from
<ul style="list-style-type: none"> • Name • Job Role • Home Address or postcode • Email Address • Gender • Marital Status • (Dependents date of birth if adding to BUPA) • Lease details (if leasing car through Electric Car Scheme) • Date of birth • Job title • National Insurance or Social Security 	<ul style="list-style-type: none"> • Directly from you

<ul style="list-style-type: none"> Number Working hours Start and Leave Dates Bank account details Salary and allowances Student loans Pension contributions Expenses and Pleo Card Transactions Details of leave including sick leave, holidays, special leave Information relating to Maternity, Paternity, Shared Parental and Adoption leave and pay. Payroll records Tax codes and tax status Nationality Residential Status 	
---	--

Oxehealth has a contractual obligation to pay employees and provide contracted benefits and a legal obligation to provide maternity pay and leave (Employment Rights Act 1996 and Statutory Maternity Pay Regulations 1986) and statutory sick pay (Social Security (Incapacity for Work) Act 1994 s8). Oxehealth also has a legal obligation under the Income Tax (Earnings and Pensions) Act 2003 to process information related to share schemes and Section 431 elections for tax compliance and reporting purposes, and a legitimate interest in processing payments for Pleo cards provided to employees.

Insurance:

To arrange insurance for company vehicles for employees under 25 we may collect and use the following information:

What Personal Data we collect and use	Where we collect your Personal Data from
<ul style="list-style-type: none"> Name Date of Birth Driving Test Pass Date Details of driving convictions or previous accidents 	<ul style="list-style-type: none"> Directly from you

Oxehealth has a contractual obligation to provide insurance for company vehicles for some employees.

Performance and Development:

To meet the training and development needs required for your role, set performance and development objectives and assess your performance, conduct salary reviews, keep records of training, carry out internal audits of onboarding and offboarding and deal with any employer / employee related disputes we may collect and use the following information:

What Personal Data we collect and use	Where we collect your Personal Data from
<ul style="list-style-type: none"> Name Job Title Email Employment start and End Date Qualifications & Training Records P&D Objectives 	<ul style="list-style-type: none"> Directly from you Your line manager Your colleagues

<ul style="list-style-type: none"> • Performance reviews • Performance Ratings • Grievance and/or Disciplinary Records (Including Meeting Notes, Witness Statements, Evidence, Investigation Records and Outcomes) • Information related to your training history and development needs 	
--	--

Oxehealth has a legitimate interest to: comply with requirements of 13485 and 27001 standards to maintain certification.; to investigate and resolve workplace issues fairly, uphold Oxehealth policies, and maintain a safe, compliant, and productive work environment; and to align employee goals with business objectives, support career development, and ensure fair and consistent salary reviews

Use of CCTV on Oxehealth Premises:

Oxehealth uses CCTV in selected areas of its premises for the purposes of physical security and access control. Cameras are positioned at entry points and within internal areas where there is a need to monitor access to sensitive infrastructure such as server equipment and stock.

CCTV may also operate in some shared office areas and access routes. Cameras are not installed in private areas such as bathrooms or meeting rooms. The system does not record sound or use facial recognition or biometric technologies. CCTV footage is video-only.

CCTV may capture employees entering, exiting, or passing through secure areas, but is not used for performance monitoring or disciplinary purposes.

What Personal Data we collect and use	Where we collect your Personal Data from
<ul style="list-style-type: none"> • Video recordings of individuals walking through or entering areas adjacent to secure infrastructure (e.g., entrance to the demo and experiment suite). 	<ul style="list-style-type: none"> • CCTV cameras located on company premises.

Oxehealth has a legitimate interest in maintaining physical security, preventing unauthorised access to critical infrastructure, and protecting its property and systems

Emergency Contacts:

To notify your emergency contact in the event you have been involved in an accident at work which requires medical assistance and to obtain permission for medical treatment where it is required we may collect and use the following information:

What Personal Data we collect and use	Where we collect your Personal Data from
Emergency contact details including: <ul style="list-style-type: none"> • Name of Emergency Contact • Relationship to Employee • Telephone Number of Emergency Contact 	<ul style="list-style-type: none"> • Directly from you

Oxehealth has a legitimate interest to notify employees next of kin in the event of an emergency and a vital interest to request consent for medical treatment.

Maintain leaver records:

To maintain records of leavers to ensure we have information for references or information we are required to keep for tax reporting we may collect and use the following information:

What Personal Data we collect and use	Where we collect your Personal Data from
<ul style="list-style-type: none"> • Name • Staff no. • Address • Job title • Date of birth • NI number • Start and end date • Notice period • Personal email address • Personal telephone number 	<ul style="list-style-type: none"> • Directly from you

Oxehealth has a legitimate interest to maintain records of staff who have left for reference purposes and to communicate relevant information relating to benefits and tax.

Investment and Listing-Related Disclosures:

In certain circumstances, we may disclose personal data of senior employees or officers to support Oxehealth's investment activities, corporate debt listings, or fiduciary administration.

What Personal Data we collect and use	Where we collect your Personal Data from
<ul style="list-style-type: none"> • Name • Job Role • Copy of Contract • Contact Details • Date of Birth • ID Documents (e.g. Passport) 	<ul style="list-style-type: none"> • Directly from you or from Oxehealth internal records.

Oxehealth relies on Legal Obligation, where disclosure is required under The International Stock Exchange (TISE) Listing Rules or fiduciary governance and compliance duties under the Companies (Guernsey) Law 2008 and Trusts (Guernsey) Law 2007 and legitimate Interests, to support investment due diligence and provide necessary information to potential investors.

Legal Advice - HR and Employment Matters

In certain circumstances, we may share personal data of employees or job applicants with our external legal advisers to obtain advice or support in connection with HR or employment law matters. This includes cases involving grievances, disciplinary proceedings, performance management, or general employment law compliance.

What Personal Data we collect and use	Where we collect your Personal Data from
<ul style="list-style-type: none"> • Name • Job Role • Contract Details (e.g. terms of employment, performance concerns) • Disciplinary or Grievance Records (where applicable) • Other relevant HR correspondence or documentation 	<ul style="list-style-type: none"> • Directly from you • From Oxehealth internal records (e.g. HR systems, line manager reports)

Oxehealth has a legitimate interest in seeking professional advice to manage HR and employment law obligations, ensure compliance with legal requirements, and protect the rights and interests of the organisation and its staff.

Additional Lawful basis for processing of special category personal information

Where the information we process is special category data, for example your health data, the additional bases for processing that we rely on are:

- Article 9(2)(b) which relates to carrying out our obligations and exercising our rights in employment and the safeguarding of your fundamental rights.
- Article 9(2)(c) to protect your vital interests or those of another person where you are incapable of giving your consent.
- Article 9(2)(h) for the purposes of preventative or occupational medicine and assessing your working capacity as an employee.
- Article 9(2)(f) for the establishment, exercise or defence of legal claims.

3. How we keep your Personal Data Secure

The security of all data held and processed by Oxehealth is important to us. Oxehealth has implemented an ISO 27001 and ISO 27701 certified information security and privacy management system which is audited to ensure that we have the appropriate technical and organisational controls in place to protect your Personal Data.

Oxehealth maintains physical, electronic, and procedural safeguards in connection with the collection, storage, and disclosure of Personal Data. Our security and privacy procedures mean that we may request proof of identity before we disclose Personal Data to you.

We have put in place procedures to deal with any suspected Personal Data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

4. How long we keep your Personal Data for

We retain employee and applicant data only for as long as necessary to fulfil the purposes for which it was collected, to meet our legal and regulatory obligations, and to support legitimate business needs.

Our general retention periods are as follows:

- Job applicant data is retained for up to 12 months after the position is filled, to allow us to contact you about future opportunities if appropriate.
- Payroll and tax-related information is retained for up to 7 years after employment ends, to meet legal and financial reporting obligations.
- Basic employment records such as name, email address, telephone number and dates of employment may be retained for up to 7 years after you leave, for business continuity purposes, including providing references and communicating relevant information (e.g. benefits or share options).

- Contracts and grievance or disciplinary records are retained for up to 6 years to support the establishment, exercise, or defence of legal claims.
- CCTV footage is retained for up to 90 days unless required longer in connection with a security incident or investigation. After this period, it is automatically overwritten or securely deleted.
- Training records related to regulatory compliance may be retained for the lifetime of the relevant medical device plus an additional 15 years, as required under medical device and healthcare regulations.
- Investor and listing-related data may be retained for up to 12 months after the completion of a funding round, or for up to 7 years after the end of a listing or fiduciary relationship, to meet regulatory and audit obligations associated with stock exchange listings and debt instruments.
- Legal advice and correspondence relating to HR or employment matters may be retained for up to 6 years from the date the matter is closed, to support the establishment, exercise, or defence of legal claims and to maintain a record of professional advice received.

In all cases, we apply appropriate safeguards to ensure data is securely stored, accessed only when necessary, and disposed of when no longer required.

5. Who your Personal Data is shared with

In some circumstances, such as under a court order, we are legally obliged to share information. We may also share information about you with third parties including government agencies and external auditors. For example, we may share information about you with HMRC for the purpose of collecting tax and national insurance contributions.

We also share your data with the following third party services or contractors for the purpose of performing certain services on your behalf. Where available links to their privacy notices are attached. Third party service providers may change and while Oxehealth endeavours to keep this list up to date as these changes happen, we request you do not rely on this but contact us using the details in section 9 (Contacting Us) for the most up to date list.

Third Party Service / Contractor	Purpose	Location
Recruitment Agencies	Provision of potential candidates for job vacancies, manage temporary or contract staff.	Oxehealth accepts applications for jobs from a number of recruitment agencies in the UK or US depending on staff location.
Courier Services	Courier equipment to new starters and collect equipment from leavers	Oxehealth uses a number of different couriers based in the UK or US depending on staff location.
Atraxa Consulting Limited	UK Payroll processing and the generation of payroll reports	Brookes Mill, Armitage Bridge, Huddersfield, West Yorkshire, HD4 7NR
JustWorks	US Payroll	P.O. Box 7119, Church Street Station, New York, NY 10008-7119
Bookwise	Sweden Payroll processing and the generation of payroll reports	Fleminggatan 20, 111 26 Stockholm

BUPA UK	UK private health insurance provider	1 Angel Court, London, EC2R 7HJ
Howden Group	UK health insurance broker	One Creechurch Place, London, EC3A 5AF
Scottish Widows	UK pension provider	25 Gresham Street, London, EC2V 7HN
Lift Financial	UK Life insurance and pensions broker / advisor	Century House, Regent Road, Altrincham, Cheshire, WA14 1RR
CBS	Baseline Personnel Security Screening	5 St John's Lane, London, EC1M 4BH
The Employment Services Partnership Limited	Advice on right to work queries and or other employment law queries	c/o Cater Leydon Millard, 68 Milton Park, Abingdon, Oxfordshire, OX14 4RX
NatWest	Banking portal through which employee salary payments are made	36 St Andrew Square, Edinburgh, United Kingdom, EH2 2YB
Scottish Widows	UK Pension Provider	100 Cannon Street, London, EC4N 6EU
MetLife	UK Life Insurance Provider	PO Box 1411, Sunderland, SR5 9RB
Cintra Global	US Payroll processing and the generation of payroll reports.	Maling Exchange Hoults Yard Walker Road Newcastle upon Tyne NE6 2HL
HSBC UK	Paying employees	1 Centenary Square, Birmingham, B1 1HQ.
RBIG Corporate Risk Services	Providing insurance for company vehicles	1 Cranberry Drive, Denton, Manchester, M34 3UL
Ravenscroft Consultancy & Listing Services	Listing Sponsor	PO Box 222, 20 New Street, St Peter Port, Guernsey, GY1 4JG
Oak Group	Fiduciary and Trustee	PO Box 282, Oak House, Hirzel Street, St Peter Port, Guernsey, GY1 3RH
ESPHR	Employment law advisors	c/o Cater Leydon Millard, 68 Milton Park, Abingdon, Oxfordshire, OX14 4RX

In addition Oxehealth uses the following cloud service providers for the processing activities outlined above or for general day to day running of the business, your data may be stored on the servers owned by these providers. Where available links to their privacy notices are attached. Third party service providers may change and while Oxehealth endeavours to keep this list up to date as these changes happen, we request you do not rely on this but contact us using the details in section 8 (Contacting Us) for the most up to date list

Software Service (click link for privacy notice)	Purpose	Storage Location	Third Country Data Transfer Mechanism
Microsoft Office 365	Distributing employee onboarding and leavers information to relevant teams. Adding and removing new	United Kingdom	Adequacy Decision (EU to UK) EU-US Data Privacy

	starters and leavers from relevant insurance plans. Sending employment and related information such as contracts, P45s, applicant rejection/offer letter emails etc to employees or job applicants. Collecting payroll data, arranging P&D or disciplinary meetings, job interviews. Provision and records of compliance training.		Framework with UK extension.
Google Workspace	Storage of employee and job applicants' records including but not limited to offer letters, signed contracts, right to work and security screening checks, payroll information, training records, performance or disciplinary reviews, recruitment records, maternity/paternity/sick leave, and emergency contacts. Provision and records for compliance training.	Europe	Adequacy Decision EU to UK and permitted by UK government. EU-US Data Privacy Framework with UK extension.
Docusign	The provision and electronic signing of employee contracts and s431 elections	United States	Binding Corporate Rules EU SCCs and UK Addendum.
The Access Group	Learning Management System (Access LMS) for the provision of compliance and non-compliance related training material and other onboarding documents.	United Kingdom	Adequacy Decision EU to UK and permitted by UK government.
Sage Payroll	Calculating tax and net pay information and producing payslips, P45s, P60s and P11Ds	United Kingdom	Sage's intra-group Personal Data Processing agreements, UK IDTA or Sage's SCCs with UK Addendum.
Zoho	Providing contact details to IT for initial IT setup, new starter onboarding and leaver offboarding records.	Europe	Adequacy Decision EU to UK and permitted by UK government.
Pleo	Providing a management platform for prepaid corporate cash cards and recording Pleo card transactions.	United Kingdom / Europe	Adequacy Decision EU to UK and permitted by UK government.
Expenseln	Processing employee expenses	United Kingdom	Adequacy Decision EU to UK
Splunk	Managing on-call rota	United Kingdom / United States	Adequacy Decision EU to UK and permitted by

			UK government. EU-US Data Privacy Framework with UK extension.
Slack	Recruitment and General business communication	United States	EU-US Data Privacy Framework with UK extension.
Dropbox	Sharing accounting and payroll documentation with Unaterra (USA) and sharing SLT and Board member contracts with Investors.	United States	EU-US Data Privacy Framework with UK extension.
Miro	Recruitment Analysis	United States & Europe	EU-US Data Privacy Framework with UK extension.
Hik-Vision	Provides a mobile application (Hik-Connect) for remote access to CCTV footage stored locally on Oxehealth servers for physical security and access monitoring.	Video footage is stored on Oxehealth-controlled servers in the UK. Streaming may be transiently routed via Hikvision-managed cloud infrastructure in Ireland (AWS). Hikvision is headquartered in China.	EU SCCs only. No UK Addendum or IDTA is in place. A Transfer Risk Assessment (TRA) has been completed, and the risk is being monitored and reviewed.
BambooHR	HR system for booking holiday, maternity/paternity and sick leave, recording staff and emergency contact details and performance or disciplinary reviews and storing employee records.	Video footage is stored on Oxehealth-controlled servers in the UK. Streaming may be transiently routed via Hikvision-managed cloud infrastructure in Ireland (AWS). Hikvision is headquartered in China.	EU-US Data Privacy Framework with UK extension.

6. Location of Personal Data

We may sometimes transfer, store, or host Personal Data with third-party service providers located outside the UK and/or the European Economic Area (EEA), including in countries where data protection laws may offer a lower level of protection than in the UK.

Where such transfers occur, we ensure that they are carried out in accordance with this Privacy Notice and applicable data protection laws. We take steps to ensure that recipients provide adequate levels of protection and security for Personal Data.

The international transfer mechanisms we rely on include:

- The UK–EU adequacy decision (for transfers to EEA countries);

- The EU–US Data Privacy Framework with UK extension (for transfers to certified US organisations);
- Standard Contractual Clauses (SCCs) with the UK Addendum;
- Or, where available, Binding Corporate Rules (BCRs).

Where none of the above mechanisms apply, we will carry out a Transfer Risk Assessment (TRA) to identify appropriate supplementary measures and ensure an equivalent level of protection.

Where third parties process Personal Data on our behalf, we require them to implement appropriate safeguards to protect that information.

7. Your Personal Data Rights

You may have certain legal rights relating to your Personal Data, subject to local data protection laws. Depending on the applicable laws these rights may include the right to:

- Access the personal data we hold about you.
- Learn more about how we process your personal data..
- Correct any inaccurate or incomplete personal data we hold about you.
- Request the deletion or erasure of your personal data where applicable.
- Restrict or object to the processing of your personal data including for direct marketing purposes.
- Obtain a copy of your personal data in a portable format or request that we transfer it to another provider.
- Opt out of certain types of processing, including the sale of personal data (note: we do not sell personal data) or sharing of your personal data for targeted advertising, where applicable under local laws.
- Not be subject to decisions based solely on automated processing, including profiling, which produce a legal or similarly significant effect on you.

To exercise any of these rights, please contact us using the contact details below. We will respond to your request as required by applicable law, typically within one month. In some cases, we may need additional time due to the complexity or volume of requests, in which case we will notify you.

Where permitted by law, we may require proof of your identity before fulfilling your request. In some cases, we may decline a request if it is manifestly unfounded, excessive, or otherwise not required by applicable law, but we will provide an explanation in such instances.

Direct Marketing

You have the right to object to the use of your personal information for direct marketing at any time. You do not need to provide a specific reason for such objection, and we will honour your request promptly.

Non Discrimination

Oxehealth respects and upholds applicable data protection rights and ensures that no unfair treatment or discrimination occurs as a result of exercising those rights.

Automated Decision Making

We do not currently engage in decision-making based solely on automated processing, including profiling, that produces legal or similarly significant effects.

8. Contacting Us

Oxehealth is registered with the Information Commissioner's Office (ICO) in the UK and has appointed a Data Protection Officer (DPO) to oversee compliance with all data protection laws in the jurisdictions in which we operate. You can find details of our registration and the data protection officer on the ICO's [register of fee payers](#).

To exercise your rights regarding your Personal Data, or if you have questions regarding this Privacy Statement or our privacy practices please email us at privacy@oxehealth.com, call us at +44-1865-900599, or write to us at:

Oxehealth Data Protection Officer
Bee House
140 Eastern Avenue
Milton Park
Oxfordshire, OX14 4SB
United Kingdom

When you contact us please indicate what country and state you reside in so we can address your inquiry appropriately.

9. In The Event You have a Complaint

We are committed to working with you to obtain a fair resolution of any complaint or concern about privacy. If you are unhappy with the way in which your Personal Data has been processed please contact Oxehealth's Data Protection Officer using the contact details above.

If you remain dissatisfied then you have the right to apply directly to the relevant supervisory authority for a decision. You may contact them as follows:

We are committed to working with you to obtain a fair resolution of any complaint or concern about privacy. If you are unhappy with the way in which your Personal Data has been processed please contact Oxehealth's Data Protection Officer using the contact details above.

If you remain dissatisfied then you have the right to apply directly to the relevant supervisory authority for a decision. You may contact them as follows:

United Kingdom

Information Commissioner's Office

Tel: 0303 123 1113

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Live chat: <https://ico.org.uk/global/contact-us/contact-us-public/public-advice/>

Website: www.ico.org.uk

Sweden

IMY - Swedish Authority for Privacy Protection

Integritetsskydd Myndigheten, Box 8114, 104 20 Stockholm, Sweden

Tel: +46 (0)8 657 61 00 (Monday to Friday 9am to 12pm)

Email: imy@imy.se

Website: www.imy.se

United States

If you are based in the United States, you may contact the following organisations:

Federal Trade Commission (FTC): File a complaint via <https://reportfraud.ftc.gov>

Your State's Attorney General: A directory of state Attorneys General is available at <https://www.naag.org>

California residents: For complaints under the California Consumer Privacy Act (CCPA), you may contact the California Privacy Protection Agency (CPPA) via their website at www.ccpa.ca.gov

10. Review and Update of Privacy Notices

Oxehealth will review and update our Privacy Notices from time to time to reflect changes in our practices, technologies, legal requirements and other factors. If we do, we will update the 'effective date' at the top of this page. We encourage you to periodically review this Privacy Notice to stay informed about our collection, processing and sharing of your Personal Data.