About us

TAC Healthcare Group Ltd ("TAC" – "we", "us", "our") is a private provider of medical care and treatment, including Occupational Health. To deliver our services to the highest standard, we must keep records about what we provide, to whom and by whom. This means we have records about the people who work for us and the people who use our services. Our company includes TAC (Medical Services) UK Limited, and we are the trading arm of TAC Healthcare Ltd. which is part owned by InHealth Group.

We take your privacy very seriously. This Privacy Notice aims to fully explain how we use your personal information depending on whether you access our service as an employee, a patient, a client, a customer or a supplier and your rights regarding that information. It includes the changes brought about by the Data (Use and Access) Act 2025 (DUAA), which amends, but does not replace, the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations (PECR).

TAC is both Data Controller and Data Processor. This means we can either decide what information we need to keep about you and why (we are the controller) or we process your information for someone else (we are the processor). We are registered with the ICO under number **ZA055225,** and TAC (Medical Services) UK Limited is registered with the ICO under number **ZA142361.**

We are committed to being transparent about how we collect and use your data to meet our data protection obligations. You can find out more by clicking any of the buttons at the bottom *or* the right of each page.

Contact us

TAC Healthcare Group Ltd. | Wellheads Crescent | Wellheads Industrial Estate | Dyce | Aberdeen AB21 7GA

Phone: 0333 0143488
Email: DPO@tachealthcare.com

We welcome your comments on any aspect of our service, including how we can improve **this** Privacy Notice . Please submit any feedback here: Speak Up Have Your Say

Services
Clients
Suppliers
Staff
Finance
Training
Quality and Compliance

Your rights
Independent advice
Data protection complaints
Lawful basis
Data requests
Why we collect your data
FAQs about your data
Marketing

Contact Details for data requests

As well as a Data Protection Officer, TAC has a Caldicott Guardian who is responsible for protecting the confidentiality of patient information and enabling appropriate information sharing. You can contact us to request for **medical records** or a **Data Subject Access Request** (DSAR).

Address

TAC Healthcare Ltd.
Wellheads Crescent, Wellheads Industrial Estate,
Dyce, Aberdeen AB21 7GA

Phone: 0333 0143488

Email: admin@tachealthcare.com

Caldicott Guardian: Dr Stuart Scott

Clinical Governance Lead: Margaret Boyd

Data Protection Officer: Wendy Sharp

Request your data

You can ask anyone at TAC for your data.

However, to make it easier, you may wish to complete our Subject Access Request Form, or you can email our DPO - details as below:

Email: DPO@tachealthcare.com

Form Link: Subject Access Request Form

IMPORTANT NOTICE – If your employer has changed OH providers, please submit Subject Access Requests to the new provider.

FAQs about your data

How do we get your personal information?

Most of the personal information we process is provided to us directly by you or at your request, for example from your GP. If you are referred to us, we can also get your information from the referrer.

Calls into our main office may be recorded with your consent and we use CCTV to monitor our premises.

We process your personal information for the following reasons:

- To provide a service
- To provide a diagnosis or treatment plan
- To deliver training
- To allow you to start working for us
- To improve the quality of our service
- To clarify events or situations and protect the safety of our staff, patients and property

How long do we keep your data?

Some records must be retained to allow us to comply with our insurance provider*, external contracts and specific pieces of legislation such as the Limitations Act 1980.

Generally, we follow the National guidance on the retention of records:

- NHS England - B1785-nhse-corporate-records-retention-and-disposal-schedule.pdf (england.nhs.uk)
- NHS Scotland : SG-HSC-Scotland-Records-Management-Code-of-Practice-2020-v20200602.pdf

***IMPORTANT NOTICE –** Our current insurance provider requires that we retain all medical records for 10 years. These records are securely archived after the retention period displayed on each service page. Access is very restricted and for insurance claims only which requires Information Governance approval. If your employer changes OH provider, all subject access requests must be made to the new provider.

Who do we share your data with?

TAC respects an individual's request to withhold information unless there is a legal requirement to disclose or hold the information (employment legislation, HMRC, Public Health etc.). There are also some cases where it is a necessary or legal requirement to process personal information even without the consent of the individual, such as exposure to substances hazardous to health .

Our clinicians may confer with their colleagues to ensure a high quality of service is provided.

Occasionally we may also use phone recordings or CCTV footage as evidence of a crime, safety event or incident involving our staff, patients or property.
If there is a claim raised against TAC we may be required to share data with our insurer.

Services
Clients
Suppliers
Staff
Finance
Training
Quality and Compliance

Your rights | Independent advice | Data protection complaints | Lawful basis | Data requests | Why we collect your data | FAQs about your data | Marketing

Why we generally collect your data

In order to provide a safe and compliant healthcare service, we need to collect and use personal information for a range of purposes. Primarily, we collect data for healthcare and administration purposes. For example, a health professional will record details such as patient's treatment as this is essential information for providing a healthcare service, including occupational health. Patient consent will be sought whether this is implied or explicit.

Other purposes for data collection and usage may include;

- Patient Records, i.e. demographics, contact details, treatment notes, results of tests/scans
- Occupational Health records for clients employees
- For insurance purposes for any claim raised against our business
- Staff Administration, i.e. pay, CV's, discipline, work management, recruitment
- Training records to ensure staff are adequately trained to carry out their role
- To investigate complaints or incidents
- To conduct Internal Audits
- To ensure the safety and security of our staff and property i.e. use of CCTV in our facilities
- Service improvement purposes, i.e. patient satisfaction survey, complaint investigations, service requests, Speak Up Have your Say
- Accounts and records, i.e. keeping accounts related to business activity, customers, financial management.
- Research papers, i.e. health or scientific research (published data will always be anonymised)
- Performance monitoring and analysis to help us assess the quality and standard of our healthcare services.
- Reporting, i.e. to commissioners, employers and registration bodies such as Healthcare Improvement Scotland and the Quality Care Commission

Profiling

- We **do not** use personal data for the purposes of any automated decision-making including profiling.

Services
Clients
Suppliers
Staff
Finance
Training
Quality and Compliance

Your rights | Independent advice | Data protection complaints | Lawful basis | Data requests | Why we collect your data | FAQs about your data | Marketing

Lawful basis

The Lawful basis
The information we gather helps ensure we are compliant with legislation and our corporate responsibility that enables us to protect our staff, patients, clients, business and property. Under the UK General Data Protection Regulation (UK GDPR), the lawful basis we rely on for processing this information is **Article 6 (1) (f)** "**Legitimate Interests**" and we process your data **for the purposes of either employment** or **of providing and delivering our services** or for **direct marketing**.

If you provide us with any information about any **reasonable adjustments** you require when attending an appointment with us, under the Equality Act 2010, the lawful basis we rely on for processing this information is **Article 6 (1) (c)** to comply with our legal obligations under the Act

Some of the data we collect is classed as 'Special Category'. Article 9 (2) of the GDPR lists the conditions we have identified for processing special category data is necessary for the purpose of:
(b) carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of **employment** and social security and social protection law
(h) preventive or **occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment

Under the DPA 2018, Schedule 1, the conditions that apply for processing special categories of personal data are:
Employment, social security and social protection
1(1) (a) the processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection

Health or social care purposes:
2 (2) (a) preventive or occupational medicine
2 (2) (b) the assessment of the working capacity of an employee
2 (2) (c) medical diagnosis
2 (2) (d) the provision of health care or treatment

Consent will always be sought to share information unless it is required in the public interest or there is a court order – in this case we will aim to inform you beforehand.

Services
Clients
Suppliers
Staff
Finance
Training
Quality and Compliance

Your rights | Independent advice | Data protection complaints | Lawful basis | Data requests | Why we collect your data | FAQs about your data | Marketing

TAC Services

TAC Healthcare

- Industrial Hygiene
- Occupational Health
- Mental Health & Wellbeing
- Physiotherapy
- Private Services
- TAC Sunbury

- Services
- Clients
- Suppliers
- Staff
- Finance
- Training
- Quality and Compliance

- Your rights
- Independent advice
- Data protection complaints
- Lawful basis
- Data requests
- Why we collect your data
- FAQs about your data
- Marketing

Occupational Health

About our OH Department

TAC Healthcare offers a wide range of Occupational Health (OH) services depending on the nature of our client's business or requirements. The type of services we offer include Workplace Medicals, Health Surveillance Screening, Management Referrals/Case Management, Substance Screening and Travel Health. Our Industrial Hygiene service sits under OH.

We work with large and small businesses across the UK and can also provide private Occupational Health services to individuals.

Information we may specifically collect for OH

- Patient Demographics, including name, date of birth, and address.
- Job title and Employer
- Information relating to reason for referral.
- Patient Records; completed patient questionnaires, treatment notes, results of tests/scans/medevacs, reports, medical certification
- Telephone recordings of consultations with patients – with consent
- Telephone recordings of calls between a Topside doctor and a Medic

Who has access to this data?

Our service is medically confidential. Medical records are securely stored in our iOH system and only accessible to members of the Occupational Health Team. Any reports to your employer only include relevant facts and opinions about whether you are medically fit to do a particular task or job, if you have a condition that may affect your role and/or whether any adjustments are recommended. If you choose not to allow your employer to see the report, they will have to make decisions based on the information they have.

All OH information is kept in iOH and access is restricted based on role and purpose to help provide you with the required OH service. IOH Client Users have access to their Employee Personal Information and medical certification and restricted access to reports.

Where you work in a safety critical role, we will need to inform your employer where we are required to by law or if it is in the public interest.

Why are we collecting this for OH?

To provide an Occupational Health service we collect and process sensitive information about your health and forms part of your occupational health record. This information can relate to both your physical or mental health and may include past and current medical history, medication that you may be taking or have taken, as well as past and current occupational health records. Depending on the service provided, under the applicable UK Legislation, we may use this information to determine your fitness to work, to identify any risks or whether you need a reasonable adjustment.

How long do we keep your data?

- OH Records (staff) - 6 years after leaving
- Health Records and Radiation dose records for classified persons - 50 years from the date of last entry or age 75, whichever is the longer
- Personal exposure of an identifiable employee monitoring record - 40 years from exposure date
- Personnel health records under occupational surveillance - 40 years from last entry on the record
- Please see - FAQs for information about archived records

Where do we store your data?

In the UK on:
Our own OH System iOH, which is an integrated Occupational Healthcare Platform

Services
Clients
Suppliers
Staff
Finance
Training
Quality and Compliance

Your rights
Independent advice
Data protection complaints
Lawful basis
Data requests
Why we collect your data
FAQs about your data
Marketing

Industrial Hygiene

About our Industrial Hygiene Department

Our Industrial Hygiene department identifies, evaluates and controls exposure to workplace hazards that may include chemicals, dust, fumes, noise, radiation, vibration and extreme temperatures, to name a few.

Often the risk from health hazards present in the workplace is not readily apparent, recognised or understood. They can cause serious ill-health over the longer term from repeated relatively low levels of exposure if appropriate controls have not been applied. You may also know Industrial Hygiene referred to as Occupational Hygiene.

Information we may collect

- Personal information, e.g., name
- Personal monitoring
- Patient Records, i.e., treatment notes, results of tests / scans/ medevacs, certificates
- Health data
- Past and present monitoring reports
- Medical history
- Job role and hazards
- Health information that would be classed as 'special category data'
- Information related to physical/sensory/mental health
- Hearing and audiometry

Who has access to this data?

Our service is medically confidential. Medical records are securely stored and are only accessible to members of the Industrial Hygiene Team. The Industrial Hygiene Team consists Industrial Hygienists, Medics and Admin.

Why are we collecting this for Industrial Hygiene?

To provide an Industrial Hygiene service we need to collect and use personal information for a range of **monitoring purposes**. Primarily, we collect data to help **identify, evaluate and control exposure to workplace hazards** that may include chemicals, dust, fumes, noise, radiation, vibration and extreme temperatures, to name a few. For example, we may record details such as your name, if you have been exposed to noise, where the monitoring took place and when; this is essential information to provide our Industrial Hygiene service.

How long do we keep your data?	Where do we store your data?
• Personal exposure of an identifiable employee monitoring record - 40 years from exposure date • Personnel health records under occupational surveillance - 40 years from last entry on the record • Please see - FAQs for information about archived records	**In the UK on:** Our own OH System iOH, which is an integrated Occupational Healthcare Platform

Services
Clients
Suppliers
Staff
Finance
Training
Quality and Compliance

Your rights
Independent advice
Data protection complaints
Lawful basis
Data requests
Why we collect your data
FAQs about your data
Marketing

TAC Sunbury

About our Sunbury Service

TAC Sunbury provides the Global and UK Travel health support to deliver a contract to a Sunbury based client. This service involves:

- Providing and managing Travel health clinic on the client site
- Managing and supporting the Global Expatriation Health Process for the client
- Managing and supporting the Medical fitness for work/travel clearance process for client Iraq based services
- Managing Trading and Shipping medicals recall service

Information we may specifically collect for our Sunbury Service:

- Personal details; including name, date of birth and address
- Next of kin details
- Travel details
- Job role
- Records of obtained consent (Verbal and written)
- Feedback

Why are we collecting this for our Sunbury Service?

The role of the contract is to manage the client's clinical risk on all aspects of travel health and make informed. This allows the client to:

- To make decisions on medical suitability for employees to travel
- To make decisions on medical suitability for employees to do their jobs
- To make decisions on medical suitability for employees to expatriate

Who has access to this data?

Data is held on a secure platform with a hierarchy of access to different levels of data.

All data can be accessed by staff at the clinic and admin support staff.

The client's health teams can access reports and certificates.

How long do we keep your data?	Where do we store your data?
• OH Records (staff) - 6 years after leaving • Health Records and Radiation dose records for classified persons - 50 years from the date of last entry or age 75, whichever is the longer • Personal exposure of an identifiable employee monitoring record - 40 years from exposure date • Personnel health records under occupational surveillance - 40 years from last entry on the record • Please see - FAQs about archived records	• All data is securely stored on the TAC Healthcare iOH System, and the Risk Register is stored on a • restricted SharePoint page. • iFit • Cority (client health system for client staff only)

Services
Clients
Suppliers
Staff
Finance
Training
Quality and Compliance

Your rights
Independent advice
Data protection complaints
Lawful basis
Data requests
Why we collect your data
FAQs about your data
Marketing

Physiotherapy

About our Physiotherapy Department

The Physiotherapy service is run by a team of experienced Chartered Physiotherapists. It offers not only physiotherapy treatment sessions but extended scope procedures such as joint injections. All appointments are scheduled to ensure patient privacy. Patient's will be asked to confirm their identity and medical history which will be stored in medical notes and secured as per Chartered society of physiotherapy and current medical practice guidelines.

Additional information we may specifically collect for physiotherapy:

- Patient demographics, including name, date of birth, and address.
- Clinical information relating to reason for attending
- Details of previous surgery, medical conditions and implants
- Pregnancy status
- Record of obtained verbal or written consent.
- Records of treatment performed and their clinical outcomes including drug administration.
- Details of onward referral to other healthcare practitioners if required.
- KPI information and patient satisfaction surveys will be sent to patients in future

Why are we collecting this for Physiotherapy?

- To provide a Physiotherapy service we need to collect and use personal information provided to confirm patient's identity and that the reason for the referral is appropriate.
- Details of previous surgery, medical history, and implants are required to ensure that it is safe for patient to have certain procedures and to highlight if they are suitable for onward referral to imaging or other medical services.
- Record of consent is required to meet medico-legal requirements.
- Details of administered substances are collected in case of possible reaction or delayed complications and for record to be noted by NHS records where appropriate.
- Report are produced to aid in patient's clinical care and identify a possible reason for patient's symptoms, including diagnosis.

Who has access to this data?

- Anyone involved in your actual treatment such as Treating Physiotherapist or Lead Physiotherapist.
- Referrers, including Consultant surgeons, clinicians, GPs, and OH doctors within TAC
- Reports requested by healthcare professionals involved in ongoing healthcare; these will only be released if patient has consented to their release.
- Private medical insurance (PMI) companies may ask for reports on patient progress and discharge for PMI funded consultations.

How long do we keep your data?

Medical notes will be stored for a period of 6 years after date of last entry or 3 years after death.

Please see - FAQs for information about archived records

Where do we store your data?

In the UK on:

- TAC Healthcare iOH system.
- Cliniko up until January 2025*

*Allied Health Practice Management Software - Cliniko

Services
Clients
Suppliers
Staff
Finance
Training
Quality and Compliance

Your rights
Independent advice
Data protection complaints
Lawful basis
Data requests
Why we collect your data
FAQs about your data
Marketing

Mental Health & Wellbeing

About our Mental Health and Wellbeing Service (MH&W)

The Mental Health and Wellbeing Service provides psychological assessment and treatment to a wide range of mental health problems. The service can be provided in clinic, on-site or remote.

The service also offers a reactive mental health support by responding to significant events across north-east Scotland. This includes Trauma Risk Management offering rapid-response trauma support for critical workplace incidents, providing immediate guidance and structure.

Additional information we may specifically collect for MH&W:

- Patient demographics, including name, date of birth, and address.
- Clinical notes per session
- Record of obtained verbal or written consent.
- Details of onward referral to other healthcare practitioners if required.
- KPI information and patient satisfaction surveys will be sent to patients in future

Why are we collecting this for MH&W?

- To provide a Mental Health and Wellbeing service we need to collect and use personal information provided to confirm patient's identity and that the reason for the referral is appropriate
- Clinical notes are necessary for best practice and in adherence with governing body mandate (BABCP)
- To facilitate continuity of medical care

Who has access to this data?

- Only those members of staff who require access to MH&W records such as the Head of MH&W or the Chief Medical Officer in his absence.
- OH Admin have access for booking and administrative purposes only.

How long do we keep your data?	Where do we store your data?
Medical notes will be stored for a period of 6 years after date of last entry or 3 years after death. Please see - FAQs for information about archived records	**In the UK on:** • TAC Healthcare iOH system.

Services
Clients
Suppliers
Staff
Finance
Training
Quality and Compliance

Your rights
Independent advice
Data protection complaints
Lawful basis
Data requests
Why we collect your data
FAQs about your data
Marketing

Private Services

About our Private Service

TAC Healthcare Ltd provides an independent healthcare service for across several specialties and include consultation, treatment and minor procedures.

The services are provided by different clinician's including consultants and specialist nurses. Specialties include, gastroenterology, ENT, aesthetics, practice nurse, gynaecology, cardiology and orthopaedics.

Additional information we may specifically collect Private Services

- Patient Demographics, including name, date of birth, and address.
- Clinical information relating to reason for attending
- Details of previous surgery, medical conditions and implants
- Record of obtained verbal or written consent.
- Records of treatment performed and their clinical outcomes including drug administration.
- Details of onward referral to other healthcare practitioners if required.
- Feedback

Who has access to this data?

- Anyone involved in your actual treatment such as Clinical nurses/HSCW and consultants.
- Referrers, including Consultant surgeons, clinicians, and GPs,
- Private medical insurance (PMI) companies may ask for reports on patient progress and discharge for PMI funded consultations and treatment.
- Booking staff to dictate letters and arrange appointments.
- If there is a complaint or query, our Clinical Director or Chief Nurse, as well as a named internal investigator may need to a copy of your records as part of their investigation.
- Pharmacy auditors.

Why are we collecting this for Private services?

To provide service users with the best clinical care, consultation and treatments, it is important information is accurate and relevant to clinical care.

We collect and use personal information to make sure the best medical care is delivered on an individual basis.

Data is also collected so accurate clinical auditing can be carried out to ensure regulatory registration and requirements are met. This helps us to **perform the contract we have with you**.

How long do we keep your data?	Where do we store your data?
• Auditing data will be stored within TAC for 5 years • Medical notes will be stored for a period of 6 years after date of last entry or 3 years after death. • Please see - FAQs for information about archived records	• Cliniko* online diary system. *Allied Health Practice Management Software - Cliniko

Services
Clients
Suppliers
Staff
Finance
Training
Quality and Compliance

Your rights
Independent advice
Data protection complaints
Lawful basis
Data requests
Why we collect your data
FAQs about your data
Marketing

Staff

Talent

Human Resources

Services
Clients
Suppliers
Staff
Finance
Training
Quality and Compliance

Your rights
Independent advice
Data protection complaints
Lawful basis
Data requests
Why we collect your data
FAQs about your data
Marketing

Talent

About our Talent Department

We are usually the first point of contact new staff have with TAC. We process personal data provided by you or former employers during the recruitment stage and for keeping records of the process. Processing data from job applicants allows us to manage the recruitment processes, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. You can see a more detailed version of our group-wide Recruitment Privacy Notice here.

Information we may collect specifically for Talent:

- The name of the companies you work or have worked for, your current role and past positions, opinions of named referees,
- Information contained in your CV, your qualifications, remuneration package and the output of interviews and conversations had with you
- Correspondence we enter into with you
- Eligibility to work in the UK before employment starts
- IP address regarding the parts of our website you have accessed Information about your health if we need to make reasonable adjustments
- Information relating to your racial or ethnic origin or political or religious beliefs.

Who has access to this data?

- Third party processors: When you apply for a position, we have advertised with a recruitment job board or agency, your application is processed by them and shared with us.
- Affiliates: We may share some or all of your personal data with our affiliates. If so, we will require them to comply with our Privacy rules.
- Corporate Restructuring. We may share personal data when we do a business deal, or negotiate a business deal, involving the sale or transfer of all or a part of our business or assets..

Why are we collecting this for Talent?

Processing data from job applicants allows us to manage the recruitment processes, assess and confirm a candidate's suitability for employment and decide whether to offer a job. We may also need to process data from job applicants to respond to and defend against legal claims. This helps us to **comply with our legal obligations**.

How long do we keep your data?	Where do we store your data?
If your application for employment is unsuccessful, we will hold your data on file for 180 days after the end of the relevant recruitment process. If you agree to allow us to keep your personal data on file, we will hold your data on file for a further 180 days, or such other period as may be required by law, for consideration for future employment opportunities. At the end of that period, or once you withdraw consent, your data is deleted or destroyed.	We will store your data in as few places as practicable to ensure the data is efficiently managed and to minimise security risks. Your data may be stored on our proprietary database, email and company servers or on paper. We will not use your data for any purpose other than the recruitment exercise for which you have applied as described in this Privacy Statement.

Services
Clients
Suppliers
Staff
Finance
Training
Quality and Compliance

Your rights
Independent advice
Data protection complaints
Lawful basis
Data requests
Why we collect your data
FAQs about your data
Marketing

Human Resources

About our Human Resources Department

Our Human Resources (HR) Department sits within People Services and is provided by InHealth Group Ltd. They support TAC manage the entire employee lifecycle and support employees in their day-to-day tasks.

They also manage Employee Relations and equip managers with the skills needed to support staff and resolve issues.

Additional information we may specifically collect for HR:

- References
- Payroll
- Absences
- Employee relations cases (disciplinary and/or grievance records)
- iTrent issues
- Role changes
- New starters/Leavers information
- Maternity, paternity and other family absences

Why are we collecting this for HR?

To manage our people service we need to maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights pay our staff and administer benefits and pensions. It also allows us to process information necessary for health or social care reasons including preventative or occupational medicine

This helps us **perform the contract we have with you** and **comply with our legal obligations**.

Who has access to this data?

Our HR Team has full access to Employee data but will not be privy to full staff appraisals unless there is an issue that requires their support.

TAC staff and managers will have access to iTrent and Inspire (LMS) via an AD account, where minimal data can be added or amended. Critical data can only be amended by People Services by formal request

How long do we keep your data?	Where do we store your data?
Data retained in HR applications align with existing HR Retention Policy in brief: Staff record: 6 years after the staff member leaves or their 75th birthday whichever is the sooner. Grievances, Disciplinary, Capability: 6 years from the data the case is adjudicated, or any appeal process completed.	HR data is stored in iTrentiTrent Payroll & HR Software, Integrated HR & Payroll App Platform | MHR (mhrglobal.com)

Services
Clients
Suppliers
Staff
Finance
Training
Quality and Compliance

Your rights
Independent advice
Data protection complaints
Lawful basis
Data requests
Why we collect your data
FAQs about your data
Marketing

Clients

About our Business Development Department

Our Business Development (BD) Department is split into Occupational Health and NHS and manages all aspect of sourcing new business opportunities and any associated tender/framework applications.

BD is responsible for ensuring all evidence is maintained in any business portal that promotes our services to current and new customers.

Additional information we may specifically collect for Business Development:

- Contracts/SLA's/PO's
- Contract Leads
- Commercially Sensitive data
- Scope of Works
- Minutes of meetings
- KPIs/targets
- Quality Plans
- Details of Complaints/Complements/Issues and subsequent investigations

Who has access to this data?

- BD Team, Account Managers and Finance can access client financial data.
- BD Team, Account Managers and admin staff can access information pertinent to contract delivery
- Quality and Compliance (Q&C) can access stats and reports to monitor that KPIs are being met. Q&C may also need to view any evidence related to complaints / investigations
- The Directors can access reports and statistical data.

Why are we collecting this for Business Development?

To provide the services that you have secure from us, it is important that we keep evidence of what has been agreed, who in your organisation has made this arrangement and what it is you have purchased.

To that end, we need to collect this data to ensure that we are delivering the contract agreed with you.

This information protects our company, our patients and clients and allows us to evidence legal compliance including with the Limitations Act 1980 and Prescription and Limitation (Scotland) Act 1973

How long do we keep your data?	Where do we store your data?
This is determined by the Limitations Act 1980 and Prescription and Limitation (Scotland) Act 1973	Your data is stored in the relevant BD site in SharePoint which has restricted access rules in place. Financial data is held in Xero, the accounting software we use.

Services
Clients
Suppliers
Staff
Finance
Training
Quality and Compliance

Your rights
Independent advice
Data protection complaints
Lawful basis
Data requests
Why we collect your data
FAQs about your data
Marketing

Suppliers

About our Procurement Department

TAC operates an internal Procurement Department, delivering services both internally and to our clients. The department sources a wide range of goods and services from approved suppliers, following a thorough compliance and vetting process. We maintain a register of all approved suppliers, which also includes the third-party Network Clinics we collaborate with.
We are committed to mapping the full supply chain for all providers working with TAC to ensure that our partners operate ethically and transparently. This approach supports our ethical responsibilities and reinforces our commitment to social values.

Additional information we may specifically collect for Procurement:

- Completed New Suppliers form / Network Clinic details
- Suppliers bank details
- Suppliers contract leads and contact details
- Requested policies
- Requested certificates
- Records of relevant staff competences and training
- Relevant staff experience/CV's
- Price lists /codes
- Supply chain history
- Records or complaints / Nonconformances
- Tender documentation

Why are we collecting this for Procurement?
We collect this information to ensure that our suppliers uphold high standards of quality and demonstrate a strong commitment to their social responsibilities.

For clients using our tender process, this supports transparency and allows us to fulfil our legal obligations to conduct thorough due diligence. This ensures that all potential partners are legitimate and not involved in activities such as money laundering or modern slavery.

Collecting this information protects our company, clients, and patients, enabling us to assess financial stability and verify that suppliers are not listed on any sanctions or watchlists.

Who has access to this data?

Our Procurement department manage all New Supplier Forms and update the Approved Suppliers List.

Personal supplier data is only available to the Supplier 'owner' in TAC and our Quality and Compliance Team.

The Approved Suppliers List is available to all TAC staff.

How long do we keep your data?	Where do we store your data?
It is a requirement of NHS England that we keep Approved Supplier records for 15 years from date of last revision. If you have been unsuccessful at tender, we will keep your data 6 years.	Supplier bank details are added to Xero, our accountancy software. At present we store your summary data on our SharePoint site in our Approved Suppliers List

Services
Clients
Suppliers
Staff
Finance
Training
Quality and Compliance

Your rights
Independent advice
Data protection complaints
Lawful basis
Data requests
Why we collect your data
FAQs about your data
Marketing

Marketing

About our Marketing Department

The marketing department is dedicated to promoting our brand and driving new traffic to our websites, running campaigns and implementing strategies to grow our lead and patients lists, nurture leads into paying customers. Alongside supporting our business development colleagues to assist with business growth objectives. Marketing will use range of digital tools and resources which handle user data once implemented

Additional information we may specifically collect for marketing:

- Personal demographics
- Enquiry summary
- Company name
- Email address (for newsletter subscriptions)

Who has access to this data?

The tachealthcare.com website is managed by our marketing team, with admin and business development receiving relevant notifications containing enquiry details where appropriate. Website subscriber data collected via MailerLite is accessible to authorised members of the marketing team for the purpose of managing email communications. Data collected via the website is retained and deleted in line with the data retention policy.

Advertising and Analytics Services provided by Others (use of Cookies)

We allow others to provide analytics services and serve advertisements on our behalf across the web and in mobile applications. These entities use cookies, web beacons, device identifiers and other technologies to collect information about your use of the services and other websites and online services, including your IP address, device identifiers, web browser, mobile network information, pages viewed, time spent on pages or in apps, links clicked, and conversion information. This information may be used by TAC to analyse and track data, determine the popularity of certain content, deliver advertising and content targeted to your interests on our services.

Why are we collecting this for Marketing?

TAC Healthcare uses online forms to gather enquiries, service requests, and email subscribers from prospects and existing clients. Submissions are collected via secure platforms embedded on our website, including Typeform for enquiries and MailerLite for email subscriptions, and are used to:

- Follow up with enquiries and process booking requests.
- Provide a simple and accessible way for clients and subscribers to tell us about their needs or sign up for relevant updates.
- Send external communications to individuals who have opted in to receive marketing or newsletter content.
- Understand demand trends and tailor our marketing and services accordingly.

How long do we keep your data?	Where do we store your data?
In alignment with our data retention policy website records will be deleted monthly.	• **tachealthcare.com** - enquiry data is collected via Typeform with main servers located in Virginia, USA. Typeform states it uses AWS infrastructure in Virginia and supports international data transfers using appropriate safeguards such as SCCs.Headquarters is Barcelona, Spain. • **Email subscriber data** - is collected via MailerLite through website subscription forms. MailerLite states that its platform complies with GDPR, its data storage centre is in the European Union, and it uses ISO 27001-certified infrastructure to protect subscriber data

Services
Clients
Suppliers
Staff
Finance
Training
Quality and Compliance

Your rights | Independent advice | Data protection complaints | Lawful basis | Data requests | Why we collect your data | FAQs about your data | Marketing

Quality and Compliance

About our Quality and Compliance Department

The Quality and Compliance (Q&C) department is dedicated to ensuring that the services we provide are consistently delivered to a high standard. As Q&C is not clinical and acts autonomously within TAC, this means that we are able to ask the hard questions to make sure services remain safe and are compliant with legislation, regulations and standards.

Additional information we may specifically collect for Quality and Compliance :

- Demographics related to feedback/complaints – names, contacts details, Date of Birth, bank details, etc
- Patient records and notes when investigating complaints or incidents
- Client contracts for quality plans
- Reports for monitoring that may include personally identifiable information
- Whistleblowing (**not** safeguarding data)
- Patient feedback – complaints, compliments
- Investigation reports
- Audit reports – services delivered, quality standards, KPIs

Who has access to this data?

Only Quality and Compliance Team and IT Administrator can 'access all areas'. NB this access does not include confidential board papers or personnel records and but does include evidence of staff training and competency and proof that all recruitment processes have been completed during onboarding.

Why are we collecting this for Quality and Compliance?

We need this information to make sure that our service is compliant with legislation and regulations. It is also important as it allows us to either respond to complaints or monitor how others have responded to identify and capture opportunities for improvement.

We are also responsible for planning and carrying out internal audits across the business so it is important that we fully understand how each speciality operates and how they meet the requirements of patients and customers, trends and issues that impact the business and our stakeholders.

How long do we keep your data?	Where do we store your data?
• Complaint records are kept for 10 years, and all other data is kept in line with the National guidance on the retention of records. • Patient records in Cliniko are archived after 5 years from last appointment.	TAC stores data in: • SharePoint • Private Patient information is stored in Cliniko • Occupational Health data is stored in iOH

Services
Clients
Suppliers
Staff
Finance
Training
Quality and Compliance

Your rights
Independent advice
Data protection complaints
Lawful basis
Data requests
Why we collect your data
FAQs about your data
Marketing

Finance

About our Finance Department

The TAC Finance department is responsible for the day-to-day financial operations of the business. This includes preparation of management accounts and reports, complying with HMRC regulations and company banking. We are the team that issue invoices for any services delivered directly to patients or to clients based on service contracts and purchase orders. We also process supplier invoices and monitor project costs.

Additional information we may specifically collect for Finance:

- Client accounts payable information
- Self-Funded Clients – patient demographics, name, address, contact and also bank details Approved Supplier Records including bank certification and bank details
- Client Contracts, Agreements and Purchase Orders
- Employee Bank Details for Payroll

Who has access to this data?

Accounts - Our Finance Team, CEO, CFO, Facilities Team, Procurement Team and key personnel who require it have access to Xero our accountancy package – access is restricted based on role and job requirement, for example to create Purchase Orders.

Payroll - Our Finance Team and Payroll Team; managers will have sight of salaries for staffing purposes only

Client data – Finance Team, Account Managers

Patients card details – Finance Team and Booking Teams for taking deposits and payment upfront via Square* (a contactless payments system).

Why are we collecting this for Finance?

- Client information – to ensure orders are processed correctly and timely payment of invoices is received.
- Patient information – to ensure we know who has received a service and can invoice them for payment or to issue a refund where necessary.
- Supplier information – to ensure compliance and ability to process supplier invoices
- Employee bank details – to allow wages to be paid

How long do we keep your data?	Where do we store your data?
All financial records are kept for the minimum legal requirement. This is at least 5 years in line with HMRC requirements.	• In Xero for invoices • Precoro for PO's • Client data - in SharePoint within the restricted access Finance folder. • Payroll information is stored in iTrent (HR system) and Sage (payroll system).

Services
Clients
Suppliers
Staff
Finance
Training
Quality and Compliance

Your rights
Independent advice
Data protection complaints
Lawful basis
Data requests
Why we collect your data
FAQs about your data
Marketing

Training

About our Training Department

Our Training Department's job is twofold. We manage the Training records for the entire company and are responsible for monitoring expiries and making sure you are properly trained and competent in your role.

We also manage an in-house Training Centre which provides medical training for medics across the industry.

Additional information we may specifically collect for Training:

- Personal Information e.g. name, email
- Training Records
- Competency Records
- OEUK Records
- Information relating to eligibility for Course (e.g. experience via CV)
- Results of Exams; test papers, practical assessment notes
- Course feedback

Why are we collecting this for Training?

Training and Competency Records are crucial in making sure staff can effectively and confidently carry out their roles within the company. Proper maintenance of records can help identify gaps or areas of exposure within the company.

This data is also crucial within our Training Centre as it ensures any potential students is suitable and qualified to undertake the course, and to ensure that they are adequately taught and examined on the any course they attended at TAC Healthcare.

Who has access to this data?

- All training records and delegate information is securely stored and is only accessible by our Training Coordinating staff.
- For the purposes of vetting suitability, our course instructors have access to any relevant training records and information needed to make an informed decision.

How long do we keep your data?	Where do we store your data?
Training Records will be maintained for the duration of staff member's employment with TAC Healthcare and will be retained for 5 years after leaving. Student details will be retained for 3 year per HSE guidelines before being destroyed.	Staff records are stored on MINTRA, a bespoke training record site with restricted access. Each staff member is able to see their own records, but only the Training Coordinators have access to all records. Training Centre Data is stored in the restricted Training SharePoint site that gives access only to the Training Coordinators and permanent members of our Instructing staff.

Services
Clients
Suppliers
Staff
Finance
Training
Quality and Compliance

Your rights
Independent advice
Data protection complaints
Lawful basis
Data requests
Why we collect your data
FAQs about your data
Marketing

Your rights

Right	Note
The right to be informed	
The right of access	
The right to rectification	for medical opinions, inaccuracy is a mistake of fact, not opinion at the time. This means that proven mistakes in medical records will not be deleted, but a correction note will be added to the record.
The right to erasure	this right does not apply where Article 9(2)(h) applies to our lawful basis for processing special category data. Our justification is the establishment, exercise, or defence of legal claims that may arise.
The right to data portability	
The right to object	
Rights in relation to automated decision making and profiling	

You have the absolute right to object to being contacted for marketing purposes.

If you would like to exercise any your rights, please contact our DPO at dpo@tachealthcare.com

Services
Clients
Suppliers
Staff
Finance
Quality and Compliance

Your rights | Independent advice | Data protection complaints | Lawful basis | Data requests | Why we collect your data | FAQs about your data | Marketing

Data Protection Complaints

What is a data protection complaint?

- a data breach that has impacted you;
- how we have responded to your Data Subject Access Request or other privacy rights request;
- how long we keep your personal information;
- the accuracy of information we hold about you;
- the security measures we have in place to protect your personal details

What is NOT a data protection complaint?

- a complaint about our service
- that although we responded to your subject access request on time, we didn't expedite it;
- an employee raising a grievance issue, whilst also requesting copies of their personal information;
- a complaint about a service issue whilst also requesting that we delete your information.

How to raise a complaint

Speak to any member of staff in person or by phone: 0333 0143488

Report it using our: Speak Up Have Your Say Form

Email our DPO at: DPO@tachealthcare.com

What to expect

1. We will ask for proof of ID unless we are already satisfied of your identity
2. We will make sure you have the 'authority' to complain if doing so on behalf of others
3. We will acknowledge your complaint within 30 days – Note: *If the last day to acknowledge the complaint falls on a weekend or public holiday, we will provide an acknowledgement on the next working day*
4. We will investigate your complaint and keep you updated
5. We will provide you with an 'outcome of investigation' response within which we will list any lessons learned and improvements identified.

Services
Clients
Suppliers
Staff
Finance
Quality and Compliance

Your rights | Independent advice | Data protection complaints | Lawful basis | Data requests | Why we collect your data | FAQs about your data | Marketing

Independent advice about data protection

For independent advice or to escalate a complaint about data protection, privacy and data sharing issues, you can contact:

Information Commissioner (IC)

Website: https://ico.org.uk

Link to Advise services: Advice services for members of the public | ICO

Helpline: 0303 123 1113

For Deaf/hard of hearing: use the BT service Relay UK app then call 0303 123 1113.

For Textphone: dial 18001 followed by 0303 123 1113