

# About us



**TAC Healthcare Group Ltd. (TAC)** 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. We are the trading arm of TAC Healthcare Ltd. which is part owned by [InHealth Group](#).

We take your privacy very seriously and 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. It also explains your rights regarding that information.

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 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:** [admin@tachealthcare.com](mailto:admin@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](#)

Thank you

Services

Clients

Suppliers

Staff

Finance

Quality and  
Compliance

Your rights

Independent  
advice

Legal basis

Data  
requests

Why we  
collect it

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](mailto:admin@tachealthcare.com)

**Caldicott Guardian:** Ken Park

**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 email our DPO directly or complete our Subject Access Request Form, details are below

**Email:** [DPO@tachealthcare.com](mailto:DPO@tachealthcare.com)

**Form Link:** [Subject Access Request Form](#)

Services

Clients

Suppliers

Staff

Finance

Quality and  
Compliance

Your rights

Independent  
advice

Legal basis

Data  
requests

Why we  
collect it

FAQs about  
your data

Marketing



# Frequently Asked Questions about your data

## How do we get your personal information?

Most of the personal information we process is provided to us directly by you.

If you are referred to us, we can also get your information from the referrer.

We are given your personal information for one of the following reasons:

- To provide a Healthcare service
- To provide a diagnosis
- To provide a treatment plan
- To provide an Occupational Health service
- To deliver training
- To allow you to start working for us

## How long do we keep your data?

Some records have to be retained in compliance with specific pieces of information 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](#)

**Please see each services information page to find out exactly how long that department keeps your data and where it is stored.**

## Who do we share your data with?

There are some cases where it is a necessary and legal requirement to process personal information even without the consent of the individual, such as [exposure to substances hazardous to health](#).

TAC respects choice and will respect 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.). We will always try to inform you if we need to share your information for legal reasons. Other than that, we will not share your information without your permission to do so.

Services

Clients

Suppliers

Staff

Finance

Quality and Compliance

Your rights

Independent advice

Legal basis

Data requests

Why we collect it

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
- 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 conduct an investigation in response to a complaint or police enquiry
- Correspondence, including letters and emails
- 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, responding to freedom of information requests.
- Research notes, 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 Health 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](#)[Quality and Compliance](#)[Your rights](#)[Independent advice](#)[Legal basis](#)[Data requests](#)[Why we collect it](#)[FAQs about your data](#)[Marketing](#)

# Legal basis

Under the UK General Data Protection Regulation (GDPR), the lawful bases we rely on for processing this information is **legitimate interests** and we process your health data **for the purposes of providing treatment or preventive or occupational medicine**.

**Some of the data we collect is classed as 'Special Category' and Article 9 of the GDPR lists the conditions we have identified for processing special category data as:**

- (a) Explicit consent
- (b) Employment, social security and social protection (if authorised by law)
- (h) Health or social care (with a basis in law)

**The conditions that apply are Schedule 1 of the DPA 2018:**

- (a) preventive or occupational medicine,
- (b) the assessment of the working capacity of an employee,
- (c) medical diagnosis,
- (d) the provision of health care or treatment

**The Legitimate interests for the processing**

The information we gather is required by us so that we can ensure we are compliant with legislation and can make decisions about your health or treatment.

**Consent will always be sought whether this is implied or explicit.**

Services

Clients

Suppliers

Staff

Finance

Quality and  
Compliance

Your rights

Independent  
advice

Legal basis

Data  
requests

Why we  
collect it

FAQs about  
your data

Marketing



# Services

Endoscopy  
Insourcing  
(Scotland)

Physiotherapy

Industrial Hygiene

Private Services

MRI

Ultrasound

Occupational  
Health

Services

Clients

Suppliers

Staff

Finance

Quality and  
Compliance

Your rights

Independent  
advice

Legal basis

Data  
requests

Why we  
collect it

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?

- 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

### 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](#)[Quality and Compliance](#)[Your rights](#)[Independent advice](#)[Legal basis](#)[Data requests](#)[Why we collect it](#)[FAQs about your data](#)[Marketing](#)

# Endoscopy Insourcing (Scotland)

## About our Endoscopy Department

We provide onsite endoscopy services at various sites on behalf of the NHS to help to reduce waiting times; this includes Gastroscopies, Colonoscopies and Flexible Sigmoidoscopies.

Depending on the location, patients are either booked by the NHS or by us directly.

### Information we may specifically collect for Endoscopy:

- Patient demographics
- CHI Number (patient NHS number)
- Communication requirements
- Next of kin
- Medical history past and present
- Medication
- Comfort scores
- Polyp images

### Who has access to this data?

Our service is medically confidential. Medical records are securely stored and are only accessible to members of the Endoscopy Team. The Receptionist/Admin Staff will only see your contact details. If you are an NHS patient we do report patient outcomes to the NHS.

### Why are we collecting this for Endoscopy?

To provide an Endoscopy service we need to collect and use personal information to ensure the best medical care is delivered on an individual basis. To do this it is important that we have up to date accurate information.

Data is also collected so accurate auditing can be carried out on the unit's performance.

### How long do we keep your data?

- Auditing data will be stored within TAC for 5 years
- NHS Track CARE and EMS data is stored for the lifetime of the patient.

### Where do we store your data?

#### In the UK on:

- NHS TRACK CARE Written document of patient name, CHI and procedure are kept within the unit.

[Services](#)[Clients](#)[Suppliers](#)[Staff](#)[Finance](#)[Quality and Compliance](#)[Your rights](#)[Independent advice](#)[Legal basis](#)[Data requests](#)[Why we collect it](#)[FAQs about your data](#)[Marketing](#)



# MRI

## About our MRI Department

The MRI service is led by a team of highly skilled, and experienced radiographers. They are supported by local Consultant Radiologists and radiography assistants (RDAs).

Appointments are scheduled to ensure patient privacy. Patient's will be asked to confirm their identity and that information provided on MRI safety form is accurate, this will be done in a confidential manner.

### Information we may specifically collect for MRI

- Patient Demographics, including name, date of birth, and address.
- Clinical information relating to reason for referral.
- Details of previous surgery, and implants
- Details of piercings and body tattoos
- Pregnancy status
- Record of obtained verbal or written consent.
- MR images produced during examination.
- Details of administered medicines and contrast agent.
- MR report of scan findings, including potential diagnosis

### Who has access to this data?

Members of our MRI Team including Radiographers, RDA and Consultant Reporting Radiologists.

Additionally, your information may be passed to referrers, including Consultant surgeons, clinicians, GPs, and Physiotherapists.

Should any images or report be requested by healthcare professionals involved in patients ongoing healthcare; these will only be released with the patients consent.

### Why are we collecting this for MRI?

This allows staff to confirm patient's identity and that reason for the referral is appropriate. The scan images and reports are produced to aid in patient's clinical care and identify a possible reason for patient's symptoms, including diagnosis.

We collect details of previous surgery, implants, and piercings etc. are required to ensure that it is safe for patient to have a scan. Equally, details of administered substances are collected in case of possible reaction or delayed complications.

### How long do we keep your data?

- Data stored on xRM, and Sectra stored for a period of 6 years after date of last entry or 3 years after death.
- Biotronics 3D-90 days
- GE MRI scanner-maximum of 90 days.

### Where do we store your data?

#### In the UK on:

- InHealth xRM, Radiology Information System (RIS)
- Sectra Medical, Picture Archiving Communication System (PACS)
- Biotronics 3D, teleradiology, PACS for reporting purposes.
- GE Hdx 1.5T MRI scanner

[Patients](#)[Clients](#)[Suppliers](#)[Staff](#)[Finance](#)[Your rights](#)[Independent advice](#)[Legal basis](#)[Data requests](#)[Why we collect it](#)[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
- Employer
- Information relating to reason for referral.
- Patient Records; completed patient questionnaires, treatment notes, results of tests/scans/medevacs, reports, medical certification

### Who has access to this data?

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

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.

### Why are we collecting this for MRI?

To provide an Occupational Health 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?

- OH Records (staff) - 6 years after termination of employment
- 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

### Where do we store your data?

#### In the UK on:

Our own OH System iOH, which is an integrated Occupational Healthcare Platform

Patients

Clients

Suppliers

Staff

Finance

Your rights

Independent  
advice

Legal basis

Data  
requests

Why we  
collect it

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 injection and PRP procedures with the support of our radiology and medical colleagues. All types of 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 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.
- Reports 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.

### Where do we store your data?

#### In the UK on:

- Cliniko\* online diary system.
- TAC Healthcare iOH system.

\*Allied Health Practice Management Software - Cliniko

Services

Clients

Suppliers

Staff

Finance

Your rights

Independent  
advice

Legal basis

Data  
requests

Why we  
collect it

FAQs about  
your data

Marketing



# Ultrasound

## About our Ultrasound Department

The Ultrasound service is run by a team of experienced Sonographers. All types of 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 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

### Who has access to this data?

- Anyone involved in your actual treatment such as Treating Sonographer.
- 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.

### Why are we collecting this for Ultrasound?

- To provide an Ultrasound service we need to collect and use personal information provided to confirm patient's identity and that 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.

### 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.

### Where do we store your data?

#### In the UK on:

- Cliniko\* online diary system.
- TAC Healthcare iOH system.

[\\*Allied Health Practice Management Software - Cliniko](#)

Services

Clients

Suppliers

Staff

Finance

Your rights

Independent  
advice

Legal basis

Data  
requests

Why we  
collect it

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.
- KPI information
- Patient satisfaction surveys will be sent to patients in future.

### 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?

- 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.

### Where do we store your data?

- Cliniko\* online diary system.

\*[Allied Health Practice Management Software - Cliniko](#)

Services

Clients

Suppliers

Staff

Finance

Quality and Compliance

Your rights

Independent advice

Legal basis

Data requests

Why we collect it

FAQs about your data

Marketing



# Staff

Talent

Human  
Resources

Services

Clients

Suppliers

Staff

Finance

Quality and  
Compliance

Your rights

Independent  
advice

Legal basis

Data  
requests

Why we  
collect it

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?

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.

### Where do we store your data?

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

Quality and Compliance

Your rights

Independent advice

Legal basis

Data requests

Why we collect it

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

### 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

### Why are we collecting this for HR?

In order 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**.

### How long do we keep 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.

### Where do we store your data?

HR data is stored in iTrent\*

\*[iTrent Payroll & HR Software, Integrated HR & Payroll App Platform | MHR \(mhrglobal.com\)](#)

Services

Clients

Suppliers

Staff

Finance

Quality and Compliance

Your rights

Independent advice

Legal basis

Data requests

Why we collect it

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?

In order 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?

This is determined by the [Limitations Act 1980](#) and [Prescription and Limitation \(Scotland\) Act 1973](#)

### Where do we store your data?

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](#)[Quality and Compliance](#)[Your rights](#)[Independent advice](#)[Legal basis](#)[Data requests](#)[Why we collect it](#)[FAQs about your data](#)[Marketing](#)

# Suppliers

## About our Procurement Department

We have a very small Procurement Department and often work in partnership with our Parent company InHealth to purchase goods and services. We maintain an Approved Suppliers List that includes details of any Network Clinics we work with.

It is our intention to map the full supply chain for all those providing a service to TAC to ensure that the companies we work with are ethical and transparent. This helps us to meet our ethical responsibilities and supports 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 data to ensure that the suppliers we work with take quality and their Social Responsibilities seriously.

If you have applied using our tender process this ensures transparency and we are legally obliged to carry out due diligence to make sure anyone we do business with is legitimate and not laundering money or participating in modern slavery.

The information protects our company, patients and clients and allows us to check your financial stability and whether you are on any sanction lists.

### Who has access to this data?

Our Finance 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?

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.

### Where do we store your data?

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](#)[Quality and Compliance](#)[Your rights](#)[Independent advice](#)[Legal basis](#)[Data requests](#)[Why we collect it](#)[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

### Who has access to this data?

The marketing data on our tachealthcaregroup.com website can only be accessed by our Marketing Team, our CEO and our Admin Team. Our tachealthcare.com website is accessed by our Marketing Team with the Admin Team being sent relevant notifications

### 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 Healthcare 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?

- tachealthcaregroup.com - Email enquiries directed to [admin@tachealthcare.com](mailto:admin@tachealthcare.com) to follow up with enquiries and process booking requests. Submissions stored on WordPress/ Elementor (web-builder backend platform).
- tachealthcare.com - Providing online access method for prospects and existing clients to inform us of their need for services, an up-to-date list of services available from TAC occupational health and training. Submissions stored on Typeform form platform which is embedded on the Webflow website.

### How long do we keep your data?

In alignment with our data retention policy website records will be deleted monthly.

### Where do we store your data?

- tachealthcaregroup.com - Elementor Ltd. is headquartered in Israel, a jurisdiction recognised by the European Commission and the UK Information Commissioner's Office as offering an adequate level of protection for the personal data of UK and EEA residents.
- tachealthcare.com - data is collected via Typeform with main servers located in Virginia, USA. They are GDPR compliant with security and privacy standards using SCCs (Standard Contractual Clauses). Headquarters is Barcelona, Spain.

Services

Clients

Suppliers

Staff

Finance

Quality and Compliance

Your rights

Independent advice

Legal basis

Data requests

Why we collect it

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?

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.

### Where do we store your data?

TAC stores data in:

- SharePoint
- Private Patient information is stored in Cliniko
- Occupational Health data is stored in iOH

Services

Clients

Suppliers

Staff

Finance

Quality and Compliance

Your rights

Independent advice

Legal basis

Data requests

Why we collect it

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 ABC?

- 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?

All financial records are kept for the minimum legal requirement. This is at least 5 years in line with HMRC requirements.

### Where do we store your data?

- In Xero for invoices/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

Quality and Compliance

Your rights

Independent advice

Legal basis

Data requests

Why we collect it

FAQs about your data

Marketing



# Your rights

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- 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](mailto:dpo@tachealthcare.com)

Services

Clients

Suppliers

Staff

Finance

Quality and  
Compliance

Your rights

Independent  
advice

Legal basis

Data  
requests

Why we  
collect it

FAQs about  
your data

Marketing



# Independent advice about data protection

For independent advice about data protection, privacy and data sharing issues, you can contact:

## Information Commissioner

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF.

Phone: 08456 30 60 60 or 01625 54 57 45

## Scottish Information Commissioner

Kinburn Castle,

Doubledykes Road,

St Andrews, Fife

KY16 9DS

Telephone: 01334 464610

e-mail: [enquiries@itspublicknowledge.info](mailto:enquiries@itspublicknowledge.info)

Website: <http://www.itspublicknowledge.info>

Services

Clients

Suppliers

Staff

Finance

Quality and  
Compliance

Your rights

Independent  
advice

Legal basis

Data  
requests

Why we  
collect it

FAQs about  
your data

Marketing

