TadPath Privacy Notice to Clients

Introduction

At TadPath we take your privacy very seriously. We understand the sensitivities of handling all confidential healthcare-related and commercial information communicated to us in addition to the general importance of keeping all personal identifiable information private. We provide this privacy notice to you to give you details of what information we collect, how we use it and how we safeguard it as well as informing you of rights you have in relation to the information we hold. This privacy notice has been prepared on, and is applicable from 30.08.2018. Please note that we may update it from time to time in order to reflect the changing nature of laws governing data protection as well as any changes in our business.

Who we are and how to contact us

TadPath is a professional medical doctor-led healthcare company that provides a medical diagnostic histopathology service as well as sales of equipments and other resources.
The admin office of TadPath is 22 Wood End Road, Harrow, HA1 3PP
The CEO and Data Controller for TadPath is Dr Paul J. Tadrous. You may contact us by email at data_controller@tadpath.co.uk

Where we get your data (our sources)

The most usual source of information we obtain about you is the information you provide us when arranging to use our services including any contract between us.

What data we collect about you, why and how we use it

Your ID. We need to know who we are doing business with and where to send and goods we provide. Your name, address, telephone and email contacts and website information is typical but we may not collect all this information from all clients. The names and contacts of people in your organisation or working in partnership with your organisation may also be stored so we know who to contact in order to help us fulfil our professional obligations to you (e.g. your practice manager details or finance office details) or if we need further information from you in relation to our business relationship with you.
Limited financial information. We will need to collect the information we require in order to receive payments from your for our services and also to pay you for your services rendered to us if you are a supplier or if we need to give you a refund. Bank or other payment details may therefore need to be stored.
Contracts. If we are providing a service to you under contract will will keep a copy of that contract including any schedules and terms and conditions.
Invoicing and admin correspondence. We will keep records of transactions and business correspondence as is reasonable for the conduct of any business.
Clinical information about your patients: Of course we need to collect and store information about the patients we make diagnoses on. For details of this information and our dealing with it please see our privacy notice for patients.
CCTV with audio recording. As part of our security measures we have on-site CCTV. Anyone visiting our sites is therefore likely to have video and audio recording of their visit made and stored for routine security purposes. These are typically only stored for about 1 month before being overwritten unless specific footage needs to be saved for longer as part of a security or police

investigation.
Service improvement and research: We are continually assessing our own performance as a quality medical service and we want to continually improve our service and the practice of medicine generally. For these reasons we may also use some of your data (suitably anonymised) for scientific or historical research, service improvement and statistical purposes.

Lawful bases for processing your data
The preceding sections have explained in plain English why we collect the data we use and what we use it for. This section, in a sense, repeats that but puts it in terms that are more directly related to the legal wording in the General Data Protection Regulation (GDPR). The GDPR says we may only process data if we have one or more 'lawful basis' to do so. These lawful bases are defined in two 'Articles' of the GDPR. Article 6 refers to any personal identifiable data and Article 9 sets out the lawful bases for processing 'Special Category Data' (this includes health-related and financial information).
As a healthcare organisation we must have at least one lawful basis from each of these articles to be allowed to collect and process data and we must also tell you what those lawful bases are in this privacy notice. We have highlighted **in bold** the parts of the terms that particularly apply to our data processing and put in brackets some examples of how this applies to our use of data. These are abbreviated and summarised passages from the GDPR. Note that these relate to our bases for processing all personal data we deal with – not just that of patients, but also of employees and business contacts. They are as follows:

Under Article 6 of the GDPR:

1. Contract - to fulfil contractual obligations (e.g. invoicing, payment processing, processing and reporting on samples) or provide pre-contractual information (e.g. to provide quotes)

2. Legal Obligation – to fulfil our obligations in relation to the law (e.g. to comply with Court orders) and professional obligations (e.g. our obligations as medical doctors registered with the GMC – see https://www.gmc-uk.org/).

3. Vital Interests - in the limited circumstances where this basis applies (e.g. a person in a coma or otherwise lacking the ability to communicate and the data processing is necessary for an urgent life saving intervention of either the data subject or someone else)

4. Legitimate interests of ourselves or people and companies we work with to provide a service to you. (This means we may process some of the data we hold for the purposes of detecting and preventing fraud, upholding our terms and conditions of service, dealing with complaints, defending ourselves from claims and for our own restricted internal marketing purposes where we feel we would like to inform you of changes to our service or offers we may have. In all cases we will restrict the amount of data we use for these purposes to the minimum necessary to achieve the purpose and we will comply with the law. You have the right to object to your data being used in any marketing activity as well as any other legitimate interest activity.)

Under Article 9 of the GDPR:

1. processing is **necessary for the purposes of carrying out the obligations** and exercising specific rights of the controller or of the data subject i**n the field of**

employment and social security and social protection law (e.g. so we can fulfil our obligations towards our employees or other parties who do work for us. This mainly relates to data we hold on people who work for us or work with us)

2. processing is **necessary to protect the vital interests of the data subject** (similar to item 3. under article 6, above)

3. processing is **necessary for the purposes of** 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 or the management of health or social care systems and services** (e.g. we need to process your data to provide a diagnosis for you – this is our main reason for existence – and this also relates to any occupational health commitments we have to our staff or others who do work for us)

4. processing is **necessary for reasons of public interest in the area of public health**, such as protecting against serious cross-border threats to health **or ensuring high standards of quality and safety of health care and of medicinal products or medical devices**, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; (this relates to using your data to provide you with a high quality health service. It includes making a diagnosis for you and also service improvement such as conducting internal audits of the quality of our care and carrying out research to continually maintain high standards and improve services.)

Profiling, automated decision making and use of cookies
We are required by law to inform you how we use your data for any of the above technical uses. However, at TadPath we do not use profiling, automated decision making or cookies. Your data is therefore not used for any of these purposes.

How long we store your data
With regards to business and financial records we will retain these for a period that is commensurate with sound business practices and this usually means for 10 years after the last completed transaction or end of contract (whichever is later).
CCTV recordings are stored for about 1 month after which they are permanently destroyed by being overwritten. An exception will occur to this if we record CCTV clips onto external media or give over CCTV disks to the police as part of a security or criminal investigation. In this case the footage in those specific clips or disks will be retained according to guidelines for security and police investigations.
Health-related information on patients will be stored according to Royal College of Pathologists guidelines

How we keep your data safe
The security and privacy of your personal information is of utmost importance to us and we employ multiple security measured to safeguard your data.
With regards to any paper request forms submitted to us with your biopsy samples – we keep these securely locked up for a minimum of 4 weeks after the final pathology report is produced then we destroy these by secure shredding. The information on these forms is transcribed onto the electronic pathology reporting system prior to destroying the paper copies and forms part of the final pathology report.
We scan and destroy other paper correspondence similarly in order to reduce the risk of

any paper documents being compromised. We only store original paper documents as may be required for legal purposes (e.g. original certificates or contracts) and these are kept in securely locked filing systems.
Regarding computer record security we also employ a multi-pronged approach.
We have a high level of physical security on our premises including high security locks on the doors with restricted access to authorised personnel only and multi-camera high resolution continuously recording CCTV in operation on site. The CCTV system is password protected with a strong password policy.
Personal and commercially sensitive information is kept on a secure server computer (running on an uninterruptible power supply and with a regular secure back up regimen to guard against unintentional data loss). Other computers in our network act as 'dumb terminals' that are used to access the main server database but do not themselves store personal data and these are not connected to the internet.
The hard disks on our server system are encrypted with a strong password. The server system itself is protected at pre-bios level by a boot-up secure password.
The server system runs a secure Unix-based operating system.
Our pathology reporting and business systems are access restricted to authorised personnel only with a separate password system.
We operate a strong password policy on our systems.
We send correspondence by secure means such as via encrypted secure email services.
We are registered with the Information Commissioner's Office and are subject to their rules and scrutiny.

Who we share your data with
In compliance with our strict duty to medical confidentiality and to the extent permitted by law we will not share your sensitive medical information with anyone other than those involved in providing your medical care and this may include other doctors, clinics, laboratories, IT and administration (e.g. secretarial) services who provide a service to us to help us provide a secure and effective diagnostic service to you.
We may need to share some general information about you (such as your ID) with people or companies that help us provide our service (such as payment processing companies, insurance companies or whoever is responsible for paying our fees in regards to the services we provide).
We may share your information with other parties if you have specifically agreed to this – for example if you have agreed to take part in research that requires the sharing of your data.
We may be obliged to share your information to third parties by law (e.g. to comply with a court order).
We may share your information with a third party if it falls into terms of a business contract whereby we sell or buy businesses or assets.
In all cases where your information is shared, only the bare minimum that is consistent with adequately achieving the specific limited purpose will be shared.
We will never share your personal information with (or sell it to) advertising or marketing or other listing agencies to use for their own purposes unless you explicitly give us your consent to do this.

Your rights in regards to your data
The data we collect and use to provide you with a high quality diagnostic service is your data and you have rights under the GDPR in regards to this data.
You have the right to contact the Information Commissioner's Office (ICO) if you have a

concern over the way we handle your data (web site address given below).
You have the right to object to us using your data in certain ways (for example you can object to us using your data for direct marketing purposes).
You also have the right to contact us if you would like a copy of the data we hold about you and you have the right to request we correct any factual inaccuracies in that data.
You have other rights in addition to the above. The law in regards to your rights is subject to some exceptions (for example, an exception to the right of erasure includes data used to make medical diagnoses). Instead of us trying to list all your rights in legally accurate detail in this policy, we feel it is better to direct you to the regulatory body in this regard so you can see the latest and more complete version of your rights with information about how to exercise them. The regulatory body is the Information Commissioner's Office and their contact details are:

For general information about your data and your rights:
https://ico.org.uk/your-data-matters/

For general contact information:
https://ico.org.uk/global/contact-us/