

Healthy Practice Cloud - Data Privacy and Security Policy

For the purposes of your GDPR / DPA compliance, Technology Tamed Limited (TTL) is a processor and the company that provides the virtual server on which your Healthy Practice system is located (IOMart) is a sub-processor. In addition, should there be a need to investigate issues with your Healthy Practice database, it may be shared with our software developer, Datarich Solutions.

Who has access to your datafile?

In most circumstances, such as for problem investigation, test upgrades or for training, only selected employees of Technology Tamed Limited will access your Healthy Practice database (datafile).

Employees of IOMart have no direct access to the patient data within your datafile.

How do we keep your datafile secure?

1. Log on to the Cloud servers is password protected, with complex passwords being employed both for administrator and clinic users.
2. Passwords are managed by TTL and clinics are requested not to save passwords as part of their logon process but to enter them each time they log on.
3. Users cannot select their own passwords, to ensure the complexity rules are conformed to
4. Clinics are requested to notify TTL without delay should they suspect any user password has been compromised.
5. Each clinic has their own file structure on the Cloud server, with only their respective users and TTL administrators having access.
6. Only specific and appropriate employees of TTL have ongoing access to your datafile.
7. Employees of IOMart are only given access to the Cloud server when a specific maintenance task is required to be carried out by them.
8. RDP sessions between client computers and the Cloud server are encrypted.
9. Any backups of your datafile are encrypted.
10. If a copy of your datafile is required by TTL for investigation purposes, it is transferred from the Cloud to our internal secure file server using RDP which provides a secure, encrypted communication channel. Our internal server is protected with a two-stage firewall and NAT and only our employees involved with Healthy Practice have access. Where a datafile needs to be sent to Datarich Solutions this is transmitted using our FTP server access to which is password protected and limited to ourselves and Datarich Solutions. Once Datarich Solutions has copied the datafile onto their secure computer, it is removed from the FTP server.
11. If a clinic has requested data be exported, the exported files will be uploaded in a secure manner, either by TeamViewer directly onto your computer or some other secure means as required.

How long do we keep your data?

1. Should you decide to move your datafile to your own computer, it will be removed from the Cloud server and any backups on TTL's servers deleted
2. Where a datafile has been copied to TTL's server for investigation, once the investigation is complete it will be removed from TTL's server
3. Where you have requested an export from your datafile, once the exported data has been given to you and confirmed to be correct, your datafile will be permanently deleted. Once we have deleted your datafile we will send you a confirmation email to this effect.

Updated June 2020

Stour Valley Business Centre, Brundon Lane, Sudbury, Suffolk CO10 7GB Telephone: 01787 881475

E-mail: contactus@technologytamed.com Web: www.technologytamed.com

Registered in Wales No. 3258159. Registered Office: Lancaster House, Sopwith Crescent, Hurricane Way, Wickford, Essex