Real Time Reception Ltd – GDPR Audit (2018)

By using a virtual reception service, you have chosen to outsource your call answering and some interaction with your customers. **You are the DATA CONTROLLER**, but you need to be assured that we, as **DATA PROCESSORS,** have systems and processes which are compliant with the newest GDPR – (General Data Protection Regulations).

Real Time Reception (RTR), answers calls on behalf of clients and sends messages by text or email containing information on patients/customers. Further, RTR create appointments for customers with specific customer information in cloud based diaries either controlled or owned by their clients, and take credit card payments for some clients.

There are several parties involved in the customer/RTR process: our receptionists, telecoms provider, call centre software provider; your calendar software, and sometimes merchant account software. Emails to you regarding customers are also subject to GDPR.

RTR

Real Time Reception Ltd do not share or sell any data regarding our clients or their customers with any other party.

- All our staff sign a confidentiality document at the start of their employment and are trained in the importance of confidentiality to customers and clients alike.
- For most of the software they access, our receptionists use an encrypted double security password system, which allows the receptionist to login to all the systems they need without knowledge of any individual password.
    - The only exceptions to this is software that is not web-based, eg the older versions of PPS and TM2. In these cases receptionists log in using a single step password.
- We have a **strict clear desk policy** -there are no pens or paper on the desk and personal belongings including mobile phones are locked into the employee's locker in the cloakroom.
- It is impossible to copy, photo or in any way gather information that they have handled during the day.

Your Customers/Patients

As a company we store very little information about your customers. In most cases the data is stored on **your** software – practice management software, online banking software or similar – and those providers will have instigated encryption and storage on your behalf.

The only exceptions to this are MyOffice users where we are the account holders. This data is encrypted during transmission and uses the latest TLS 1.2 security protocol[i].

DATA SUBJECTS (patients, customers, callers) are entitled to access any data we have and receive copies.

- In the case of RTR this would be the recorded messages on voicemails and the call recordings when we speak to clients. Prior to initiating a discussion between a Receptionist and a potential/new/existing customer they should be informed that a recording of the call

will be made for quality and training purposes. We do this with a recorded welcome message on the line when they call in, before they get through to a receptionist.

- Recorded conversations are stored for 2 months on the server of our Telecoms provider and are protected by an IP firewall[ii] which allows access by us and by them. **If your customer requested a copy of this call within 2 months we will send a copy electronically.**
- When a call goes to voicemail the voicemail is emailed to us as a discreet file. Once it has been actioned it is stored for 4 months then deleted off the server. These are saved on our exchange server and protected by SSL. **If your customer requested a copy of this message within 4 months we can send it electronically.**
- There will still be a record that a call occurred and the outcome of the call, eg a booking or cancellation.

In addition, the caller should have a reasonable expectation of the use of any personal data collected or recorded. For example: When making a booking they will be asked to supply; Name and contact details and there would be a reasonable expectation that the data would be used for the explicit purpose for which it is collected only, ie. communication or ensuring the correctness of any appointment. Further that such data would be deemed confidential. (See previous para regarding training).

Payment Card Industry (PCI) Compliance

We take credit and debit card payments for some of our clients. The security measures mentioned above go partway to covering the requirements of PCI. Additionally, during a call we pause call recording while we take the card details. Once they are entered we can no longer see them. There is no record of the card details stored in the saved recording, and this recording is deleted at 2 months.

RTR's Clients and Prospective Client Enquiries.

- When we speak to enquirers we collect contact information directly from them, name, phone number and email address. This is entered into an excel sheet and into our Customer Relationship Management Software which is encrypted.
- If the enquiry goes further we will collect more information about the practice – fees, appointment types. This information is largely in the public domain, and is entered into call centre software so that it pops up onto the screen when there is an inbound call. This software also saves information about messages sent to you and a record of the disposition of any actions we have made for you. This information is saved in a 'single dedicated Virtual Machine instance with Amazon's EC2 shared infrastructure environment and password protected.'[iii]
- Once you are a client we will enter your banking details into our accounting software which is protected by SSL and password protection and encryption.
- Each month, at the time of billing this information is used to create the invoices and then uploaded on a spreadsheet, through an SSL secured portal to FastPay, who collect the monies on our behalf.
- Our files and any documentation in them are saved on a remote, encrypted server and password protected.
- Paper copies of documents - contracts DDM etc are stored under internal security protocols. These are kept for 6 years after the client has left us.

We are ICO registered and our registration number is Z1902894

[i] Transport Layer Security (**TLS**) and its predecessor, Secure Sockets Layer (**SSL**), both frequently referred to as "**SSL**", are cryptographic protocols that provide communications security over a computer network.

[ii] Firewalls are also used for Network Address Translation (NAT). This allows a network to use private IP addresses that are not routed over the Internet. Private IP address schemes allow organizations (or even household networks) to limit the number of publicly routed IP addresses they use, reserving public addresses for Web servers and other externally accessed network equipment. NAT allows administrators to use one public IP address for all of their users to access the Internet - the firewall is "smart" enough to send the requests back to the requesting workstation's internal IP. NAT also allows users inside a network to contact a server using a private IP while users outside the network must contact the same server using an external IP.

[iii] Amazon Elastic Compute Cloud (Amazon **EC2**) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers.
Amazon **EC2's** simple web service interface allows you to obtain and configure capacity with minimal friction.