MJog Data Security Statement

MJog Limited takes data security very seriously and are committed to protecting any information entrusted to us by all our clients to ensure confidentiality.

MJog enforces strict security procedures and maintain high levels of data protection that conforms to NHS Information Governance guidelines and Data Protection Legislation in the UK. Working with market leading suppliers we have:

- Own N3 connection (ODS number 8HL93)
- 100% IGSoC rating
- ISO 27001:2013 accredited (C1/155921S)
- GPSoC-r Lot 2 contracted supplier

We are registered with the Data Protection Register (number Z109053X) Further information on the Data Protection Register can be found at the ICO (Information Commissioner's Office) web site, or by contacting us on 01353 741641.

The MJog messaging software is pre-tested and verified to conform to the terms and conditions of long-term Partnership Agreements with the suppliers of leading clinical systems. This ensures that MJog operates to the same high standards for the protection of data. MJog is installed onto your chosen computer under the supervision and control of your staff and will be protected with a username and password chosen by you.

During the normal operation of the MJog service, your messages will be transferred from your PC to either the relevant NHS servers or to the Mobile Network via our MJog Servers (dependent on the tariff you have subscribed to).

Once MJog is installed and actively sending messages, our staff can only gain access to your MJog system with your permission, whilst under observation of your staff and for the purposes of support and maintenance.

Your patient messages (e.g. appointment reminders) will require at least the patient’s mobile number and the date and time of their appointment. You always have complete control over the content of messages and can therefore limit or exclude any personal identifiable information. You can also control which of your patients (or clients) will receive messages using implied opt-in and opt-out settings in support of information governance policies.

The transfer of all messages is protected using industry standard SSL with 256 bit encryption to ensure their safe transit. Our security validation certificate was issued by Geotrust and we have been verified by them as bona-fide.

MJog will not access any sensitive information about your patients (or clients) without your consent or knowledge. Whenever any of our staff needs to be exposed to confidential information, they will be instructed that such access is to be supervised by you, kept to a minimum, and confidential information disregarded. MJog will never use any data for any other purpose except for the delivery of messages. Nor will we divulge any mobile numbers or message details to anybody for any purpose unless required to do so by law.

If you have any further queries, send us a question at info@mjog.com