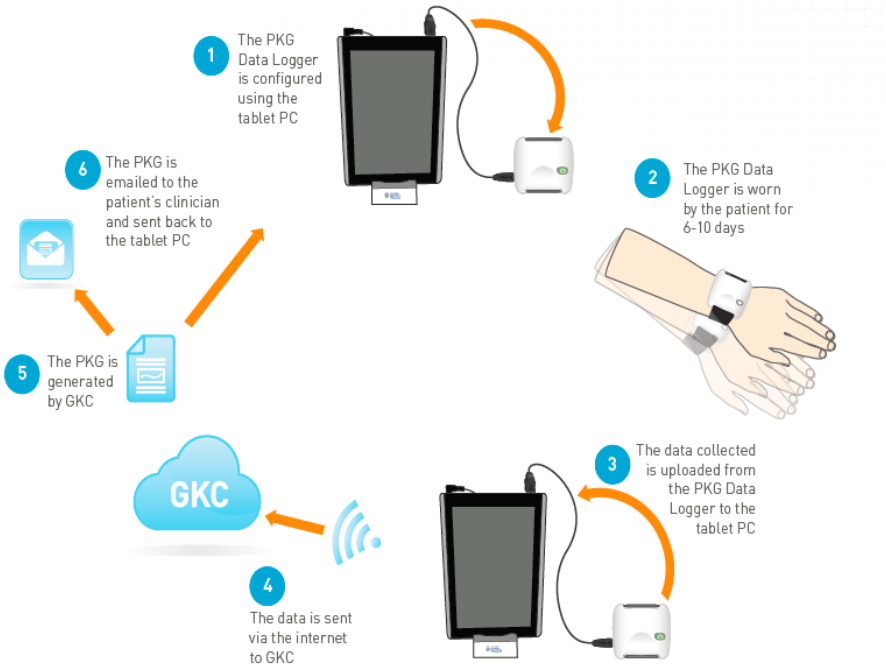
Global Kinetics Corporation

Data Security– Parkinson's KinetiGraph System

How does the PKG System work?

The Parkinson's KinetiGraph™ (PKG™) System is standalone in so far as it does not require installation of software or any physical connection of hardware onto a hospital network or machine.

A data logger is configured via the tablet and worn by a patient for 6+ days. When the data logger is returned to the clinic, data is transferred from the logger to the tablet. The tablet uploads the data file to GKC's cloud based service ('the server') for processing. The results of the processed data, the PKG, is emailed as a PDF. A copy of the PDF is downloaded to the tablet for convenience.



The tablet contains the PKG Clinic App whose function is to program a data logger, extract the data file from the logger at the end of a recording and send the data file to the server for processing and PDF generation. The tablet requires connection to a private WiFi network for transmission of data. Public or guest networks requiring browser based authentication are not acceptable since use is restricted via KNOX (Samsung's defense-grade mobile security platform)[1] to the PKG Clinic App only and not an internet browser.

What is the PKG System's medical device status?

The Parkinson's KinetiGraph System is a Class IIa medical device according to the European Medical Device Directive (MDD)[2]. It has been listed on the Australian Registry of Therapeutic Goods (ARTG) and has FDA Clearance as Class II.

[1] *White Paper: An Overview of the Samsung KNOX™ Platform* (February, 2016)

[2] Article 1 of European Council directive 93/42/EEC.

Is the data secure?

Yes, in transit the tablet uses SSL encrypted endpoints using the HTTPS protocol for transmission between the tablet and the server.

The PKG complies with data protection requirements defined in MDD 95/46/EC and stringent cybersecurity requirements established by the FDA[3]. Patient identifiers (where used) are maintained in encrypted form.

The integrity of data is protected by a series of checksums that are recorded by the data logger and checked during analysis.

Privacy of identifying information is protected by encryption. The identifying information (the patient's name) is encrypted (using a per-clinic key) by the tablet at the time that the data logger is configured. This information remains encrypted during transmission and in storage and is only decrypted at the last step of processing just before the PKG is sent to the clinician after which is promptly removed. The copy of the PKG kept on file on the server does not contain decrypted identifying information.

The credentials used by the server to process the data are generated on a per-session basis by a separate security policy server. The credentials used to analyse a data logger recording have permission only to read the data and store the results for that recording and expire automatically after 1 hour.
The credentials used by GKC engineering and support staff to access the data store are protected by multi-factor authentication tokens.

Where is the server located?

GKC's Amazon Web Services (AWS) secure cloud based platforms are regionally located according to the location of the clinic, i.e. European data does not leave Europe.

What patient information does GKC collect?

Clinics provide limited patient details to GKC to allow for the monitoring of patients. Patient details can be limited to patient initials and year of birth.

What if the tablet is lost or stolen?

The tablet is controlled centrally by GKC using Samsung KNOX mobile security. If GKC is notified that a tablet has been lost or stolen, the tablet can be remotely reset to factory defaults. Security credentials for that tablet can be revoked. The clinic is responsible for storing the tablet in a secure location.

The credentials used by the tablet to upload information to the server have permission only to upload the required data files for a particular clinic and do not have general access to the data store.

Where is the PKG PDF emailed from?

The PKG is emailed from pkg@globalkineticscorp.com. If this is blocked by the hospital mail system, clinicians will not receive the PKG.

Please contact your local GKC representative if you have any questions.

[3] 21 C.F.R. § 820.20; FDA, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff* (October 2, 2014).