Data Encryption

Users of CAT4 are responsible for the safety of the extracted data just as they are responsible for any other patient data collected in a clinic. To minimise the potential for misuse of the extract files CAT4 has a number of data security features built into it:

When the practice staff presses the ‘Collect’ Button in CAT4, to create a report, two files are produced. The two files produced by CAT4 are encrypted to ensure the data can only be viewed within CAT. A de-identified data file can be created within CAT4 using the ‘de-identify dataset’ tool. This is the only data file that can be exported and taken off-site by

- using the CAT4 'Send To' function (recommended) - full details are here: Sending data

This is recommended as it:

- provides password protection and encryption options so the file can be sent securely,
- keeps a history log of where and when the file has been sent and by which user login, and
- ensures that the practice has control over sending the file.

Patients who have withdrawn their consent to share data can be flagged in CAT. This will remove them from the de-identified data file. For details see here: Patient Consent Withdrawn - Opt Out