DATA SECURITY

In order to comply with the General Data Protection Regulation (GDPR) (*Regulation 2016/679/EU)* the data collected by the European Cystic Fibrosis Patient Registry (ECFSPR) must be pseudonymised, i.e. the patient must not be identifiable. To facilitate the data-entry process, however, it is advisable that individuals can be recognised by the person entering the data. For this reason, the ECFSPR data collection platform allows the operator in the cystic fibrosis (CF) centre to record and see the full name of the patient when a centre-specific password, created by the CF Centre Administrator, and known only to authorised users of the CF centre, is typed when entering the data but generates a unique, 6-digit patient code that is the only identifier transmitted to the central ECFSPR database. Data are encrypted (i.e. not de-codable) when transmitted.

Data Storage and System Security

- The ECFSPR database is protected in accordance with the European Data Protection legislation, physically and technically, and backup is secured. There are strict rules for de-identification of data and user.
- The name of the system used for secure storage of patient data is Host-Proof Storage: To protect the privacy of the patient the patient identifying information (the real names or other identifiers) is separated from patient clinical data in the software. This separation is maintained throughout the system.
- Patient identifying information consists of a single message per patient called the Patient Label. The Patient Labels are hashed (encrypted) and only the hash codes are stored.
- The Patient Label is linked to the patient in the browser only, and ONLY authorised users from a centre can decrypt the identifying information. It is not possible for either the Registry or the software company, who developed and maintains the data-collection software, to decrypt the identifying centre patient data.
- Identifying information is limited to the minimum required to safely identify the patient. Identifying information is linked to the patient data using the Centre Patient Code, assigned by the data collection platform or the CF centre, different to the 6-digit patient code transmitted to the central ECFSPR database.
- All data are secured in transit using HTTPS level encryption.
- The Labels File is encrypted using an algorithm called "Corrected Block TEA". Only this algorithm is fast enough to decrypt the password protected file on every page load.

The ECFSPR and OpenApp, the software company, have done as much as is reasonably possible to develop a secure software to protect data – both during transmission and after it has reached the Registry's database – and to ensure anonymity of patients. The ultimate level of security with regard to data protection and management of patient identifying data, is at centre level. Responsibility lies with the Centre Administrators and any users that have been authorised to use the data-collection software.