Standard Operating procedure (SOP)
Data protection security breach incidence handling

1. Purpose of this document

This SOP applies in case a security breach is noticed, and describes the actions needed to control the damage and prevent further spread and future incidents.

2. Definitions

Centre

The Cystic Fibrosis centre that submits Cystic Fibrosis patient data to the European Cystic Fibrosis Patient Registry (ECFSPR).

Centre Administrator (Centre Admin.)

The natural or legal person, who is in charge of the centre's CF registry and who is responsible for the management of ECFSTracker in the centre and for submission of the data to the ECFSPR (either directly or via the Country Coordinator). The Centre Administrator can add and edit users.

Country Coordinator

The natural or legal person, who is in charge of the national CF registry and who is responsible for the management of the national data, and in some countries for the submission of data to the ECFSPR. The Country Coordinator can add centres.

Data Controller

The person is responsible for storing and handling the data according the Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 as well as Danish and Italian data protection legislation.

Data Processor

Any person who works with data.

Data Protection Officer

The person responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements

Executive Committee (Exec. Com.)

Elected representatives from the Steering Group, in charge of monitoring the ECFSPR activities.

Executive Coordinator (Executive Coord.)

The person who provides a central role for information exchange, project coordination, management of sensitive timelines and general administration in the ECFSPR.

Service Desk

The Service Desk assists the centres in the use of the data-collection program, controls the data flow of the centres and national registries to the ECFSPR, and manages communication between the ECFSPR and the centres.

Software company (Software Co)

The software company in charge of developing the data-entry/upload software for the ECFSPR.

Steering Group

Consists of persons representing their country.

UNIMI

The University of Milan, in charge of data management and statistical analysis of ECFSPR data.

User

The person from a centre who is handling patient data and inputs the data into the ECFSPR dedicated software system.

3. Responsibilities

It is the responsibility of the ECFSPR to inform all users within the countries, including Centre Administrators and Country Coordinators, its own staff and the software company of this procedure. The responsibility for completing the individual steps of this procedure is identified in the column "Responsibility" of section "5. Procedure".

4. Documents needed for this SOP

NA

5. Procedure

Step	Action	Timing	Responsibility
1	**Stop the breach, including prevention further secondary spread:**		
a	Anyone inside the ECFSPR organisation, including all data processors, who are informed of or suspect a breach of security must take immediate action to prevent further spread of data.	ASAP, within the day	Users, Centre Administrators, Country Coordinators, ECFSPR personnel, Software co.
b	Each data processor with direct responsibility of storage of data is required to work immediately within his/her organisation to stop the breach.		
c	Also persons who are not directly responsible for storage of data must contact the ECFSPR Executive Coordinator immediately and inform about the breach.		
d	The Executive Coordinator contacts the data processors for identification and closure of the breach.	Asap	Executive Coord.
2	**Assess the damage and report to the ECFSPR Executive Coordinator:**		
a	After closure of the breach, the data processor must assess the damage and report to the ECFSPR Executive Coordinator with a status report of the breach, including which data were exposed and how and which measures have been undertaken to stop the breach.	Same day	Users, Centre Administrators, Country Coordinators, ECFSPR personnel, Software co.
b	The ECFSPR Executive Coordinator then immediately contacts the ECFSPR Executive Director, the ECFSPR Data Controller and the ECFS Data protection officer.		Executive Coord.
c	In case of the unlikely event of release of person-identifiable data, the centres/countries involved must be informed of the breach.	Asap, within 2 working days	Executive Coord.
3	**Report to the Danish Data Protection Agency.**		
a	The Data Controller reports to the Danish Data Protection Agency (DDPA) by phone. The phone report will be followed by a written report, which includes the further analysis of the breach and planned prevention later, as agreed with the DDPA contact person.	5 working days	Data Controller
4	**Analyse breach and develop plan for further action to prevent reoccurrence.**		

a	The ECFSPR data controller, data protection officer and executive committee perform an analysis based on the reporting from the data processors and undertake steps to prevent future incidences.	1 month	Data Controller, DPO, Exec. Com.
b	Produce a written summary of the analysis, including a plan for further action to prevent future incidence		Data Controller, DPO, Exec. Com.
5	**Report to Steering Group**		
a	The incidence analyses report is sent to the ECFSPR Steering group within one month of the incident.	1 day	Executive Coord.