Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Home Affairs (FDHA)
Federal Office of Public Health (FOPH)
Communication and Campaigns Division

Factsheet:

Date: 28 June 2023

Electronic patient records and data security

Data protection and security are crucially important in electronic patient records (EPR). The Data Protection Act (FADP) and Federal Act on the Electronic Patient Record (EPRA) ensure that this is the case. Like organisations that issue electronic identities and healthcare facilities, (core) communities can only obtain certification if they fulfil strict conditions. Checks are regularly made to verify compliance with these conditions. This is to ensure that the documents held in EPR are protected against unauthorised access and archived **securely**.

Certification according to EPRA

The technical specifications and security requirements for the EPR are prescribed by law.

Only certified core communities can use the official logo to signify that they are a trustworthy provider that complies with all federal requirements.

The technical and organisational criteria that (core) communities must fulfill to obtain certification comprise more than 400 points, approximately one hundred of which concern data protection and security. Organisational security criteria focus primarily on staff training and the appointment of security officers.

Access ID

Anyone contributing to an EPR – patient, healthcare professional, assistant or representative – must be able to log in securely using a unique electronic identity. The two-factor authentication and security level used are similar to those used for online banking. (Core) communities are required to check the identity of healthcare professionals and their assistants who are participating in the EPR scheme.

Access history

The name of everyone who has viewed EPR documents and the date on which they consulted data or added new documents are recorded in the EPR. Access journal data are available to consult for a period of ten years, during which they cannot be deleted. The access journal provides a way of detecting and prosecuting abuses.

Further information:
Federal Office of Public Health, Communication, www.bag.admin.ch
This publication is also available in French, Italian and German.

Encrypted data storage in Switzerland

The data stored in EPR (including all safeguards) are encrypted and stored by Swiss-based companies that are subject to national law. These companies are not authorised to use the data for other purposes and foreign authorities cannot oblige them to share them**.**

Secure communication

Together, the (core) communities and affiliated healthcare facilities constitute an encryption-protected trusted space. This secure space is regularly verified using vulnerability detectors. Each (core) community has a security incident management process that it can apply if irregularities occur.

Further information:
Federal Office of Public Health, Communication, www.bag.admin.ch
This publication is also available in French, Italian and German.