25 MAY 2018

GDPR

Impact on diabetes data management

The strict provisions of the General Data Protection Regulation (GDPR) apply since 25 May 2018. In future, data protection law infringements will be sanctioned with heavy fines.

The new regulations also have a massive impact on digital diabetes management. The currently available solutions comprise various risks and obligations with regard to data protection laws.

The strict provisions of the General Data Protection Regulation (GDPR) apply since 25 May 2018.
Heavy fines may be imposed in the event of data protection law infringements or non-compliance with legal obligations.

The new regulations also have a massive impact on digital diabetes management. Such solutions are available either as software that saves on a local medium or as an internet-based cloud application. These have massive differences with regard to data protection requirements:

Solutions in which no data leaves the practice/clinic are still rather unproblematic. However, if patient data is transferred to the Cloud (= to a manufacturer/third party), then one should be aware of the considerable risks and associated costs for legally compliant use.

What many practices are not aware of is that when using a cloud solution, it is generally mandatory to create and proof an extensive "Data protection impact assessment" according Art. 35 GDPR !

DIABASS® PRO (local application)

All data is stored locally;
no data will be transmitted to third parties.

- No separate clarification required
- No separate consent required
- No requirements which go beyond existing data protection obligations
- No danger to violate medical secrecy
- No internet connection required
- No data protection officer required
- No dependence on third parties
- Simple creation/restoration of backups
- Legally compliant fulfilment of archiving and documentation obligations is simply possible thanks to storage on local media
- No need to outsource data: even large volumes of data "fit" on a standard USB stick*

* Example calculation: 2000 patients with CGM data for more than 10 years. Required storage = approx. 30–50 GB

Web-based applications (Cloud)

Patient data is transmitted to device manufacturers or third parties and saved by them. They can view and make (concurrent) use of the data.

- Extensive "Data protection impact assessment" according Art. 35 GDPR is required.
- Comprehensive clarification to the patient necessary
- The patients' autonomous consent is required
- Data transfer must also be necessary for medical purposes (Art. 5 para. 1b GDPR)
- High risk of criminal liability according to violation of medical secrecy
- In case of problems with the internet connection/accessibility: working is not possible
- Creation/restoration of backups depends on the provider and/or is time-consuming
- Legally required requirements for archiving and documentation are difficult to meet
- Potential joint liability in the event of data protection infringements by the provider
- The transfer of patient data to manufacturers is problematic with regard to professional and competition laws

---

DIABASS® PRO offers security: all data remain stored exclusively on the doctor's system. No patient or usage data is transferred to the Cloud or manufacturers.

With regard to data protection requirements, there are therefore no special considerations going beyond the existing data protection obligations in the practice.

In contrast to the so-called **"Cloud"**, it is therefore not necessary to provide patients with clarifications on data transfer and to obtain legally compliant consents in advance. Neither does the use of DIABASS® PRO require the appointment of a data protection officer.

The latest version of DIABASS® PRO not only relieves physicians from administrative expenses while minimising the risk of fines, but it also supports them in fulfilling their general data protection obligations. For instance, all you need to do is press a button to create a structured copy of their data (according to Art. 20 GDPR) when they request it.