VFTH e.V.

smart medication™

Impact of GDPR (DSGVO) on smart medication™ electronic patient diary

A. Rösch, D. Schmoldt, W. Mondorf, R. Fischer

Background:
May, 25th 2018 the GDPR (English: General Data Protection Regulation, German: DSGVO - Datenschutz-Grundverordnung) was coming into effect throughout the European Community. It is shown how the new regulation impacts the smart medication™ platform in respect of data processing of personal health information.

Method:
The newly introduced GDPR was applied to the smart medication™ platform. The new law does not only emphasise on extensive protection of personal data (privacy by design) but also and for the first time includes information security (security by design) as a mandatory part within the regulation. IT security so far was not mandatory part in the preceding national law of the Federal Data Protection Act (German: Bundesdatenschutzgesetze (BDSG)).

Results:
The following key issues of GDPR were applied:

- lawful basis for processing personal health information
- measures for responsibility and accountability
- data protection by design and by default
- use of pseudonymization whenever possible
- right of access for patients
- right to erasure if requested by patient
- records of processing activities
- assignment of dedicated Data Protection Officer (DPO)

Lawful basis for processing personal health information
Legal basis for processing and storing personal health information is given by the Transfusion Act, §14 (German: Transfusionsgesetz §14): “Blood products and plasma proteins [...] shall be immediately documented by the treating physician or under his responsibility […]”. Documentation shall include patient identity (i.e. patient ID or name), factor product, batch number, dose as well as date and time of application.

Measures for responsibility and accountability
Measures for responsibility and accountability are controlled contractually by a dedicated Data Processing Agreement (German: Auftragsdatenverarbeitung).

Data protection by design and by default
In particular privacy by design (see FIG 1), privacy by default as well as pseudonymisation were established in smart medication™ right from the beginning when the platform was established in 2012.

FIG.1 Elements of Privacy by Design

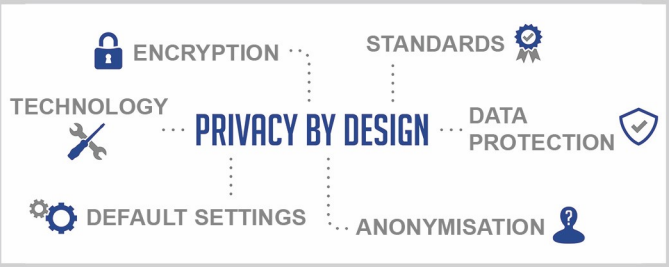

FIG. 2 General Data Protection Regulation (GDPR)

By default, smart medication™ is pseudonymized. In particular no patient name or address is stored. To protect patient identity to any other party smart medication™ is implemented using HTML5 technology. HTML5 allows distribution of the smartphone apps without using well known app stores of i.e. Apple or Google.

By default, patients do not need to provide additional personal data when using smart medication™. However, in the case patients wish to use password recovery option or like to be notified by email or SMS, they may agree to provide their email address or phone number. The usage of email address or phone number is strictly limited to this functionality.

Use of pseudonymisation whenever possible
smart medication™ is based on complete pseudonymisation of patient data. I.e. patient identification is realized using a unique patient ID (5 digit number). Personal data like patient name and address is not stored in the system. Only the attending physician can assign the patient number to a specific patient name.

Right of access for patient
At any time patients can access data provided to the system using the smart medication™ self-service web portal. Furthermore, patients may download and archive their diary e.g. in an Excel spreadsheet format.

Right to erasure if requested by patients
Erasure of all data is guaranteed in the declaration of consent signed by patient and physician before access to smart medication™ is given.

Records of processing activities
All activities of any person with access to smart medication™ are logged in audit trail database tables. Furthermore, an ISMS (Information Security Management System) based on IEC/ISO 27001 is applied to ensure information security.

Assignment of dedicated Data Protection Officer (DPO)
A dedicated DPO is assigned and documented in Data Processing Agreement of smart medication™.

Conclusion:
GDPR emphasizes on privacy by design and privacy by default as well as security by design. When processing personal health information these issues (beside all others) are important quality criteria for medical software like smart medication™.