Ensuring information security for the electronic patient diary smart medication™ by applying an Information Security Management System (ISMS) based on the international standards ISO/IEC 27001 and ISO/IEC 27799
A. Rösch, D. Schmoldt, W. Mondorf, R. Fischer

Background:
Cybercrime and cyberattacks increasingly threaten information security, data privacy and data security of medical apps and medical app platforms. The series of ISO/IEC 27001 and its supplement ISO/IEC 27799 for health IT-systems are broad in scope and cover more than just privacy, confidentiality and technical and cybersecurity issues. They are applicable to organizations of all shapes and sizes, assess information risks and treat them according to their needs.

Results:
It is shown how security controls and principles defined in the ISO/IEC 27001 and 27799 series are applied to the smart medication™ platform and how patients with hemophilia using this platform benefit from IT security measures. Furthermore, it is demonstrated how a PDCA (Plan-Do-Check-Act) iterative cycle ensures to keep up with constantly changing threats in cybercrime.

Methods:
ISO/IEC 27001 and ISO/IEC 27799 provide general IT security controls as well as health specific controls together with implementation guidances. In total 14 areas, i.e. „Information security policies“, „Access control“ or „Cryptography“ are addressed. The security controls and recommendations of the ISO standards have been analyzed and implemented to the smart medication™ platform to ensure a maximum of data security and data privacy for patients and HCPs.

Conclusion:
The international standards for information security management based on ISO/IEC 27001 provide best practice recommendations on information security management. Platforms like smart medication™ for treatment of patients with hemophilia benefit greatly when best practices of these standards are applied.