VFTH e.V.

smart medication™

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.

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.

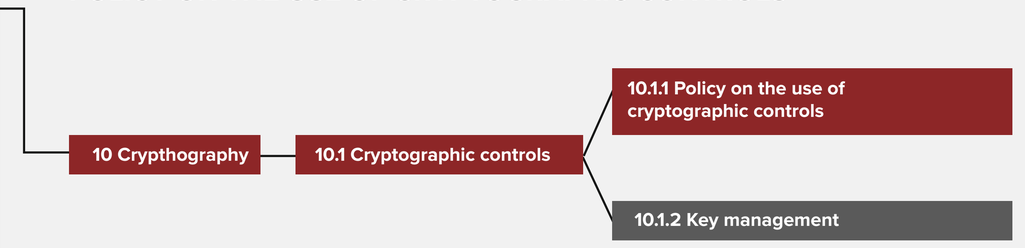
FIG. 1 STRUCTURE OF IT SECURITY CONTROLS IN ISO/IEC 27001/27002 AND 27799

FIG. 1 DETAILED STRUCTURE, OBJECTIVE AND HEALTH SPECIFIC IMPLEMENTATION GUIDELINES FOR CONTROL **"USER REGISTRATION AND DE-REGISTRATION"**

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

Health-specific control
Access to health information systems that process personal health information shall be subject to a formal user registration process. User registration procedures shall ensure that the level of authentication required of claimed user identity is consistent with the level(s) of access that will become available to the user. User registration details shall be periodically reviewed to ensure that they are complete, accurate and that access is still required.

FIG. 1 DETAILED STRUCTURE, OBJECTIVE AND HEALTH SPECIFIC IMPLEMENTATION GUIDELINES FOR CONTROL **"POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS"**

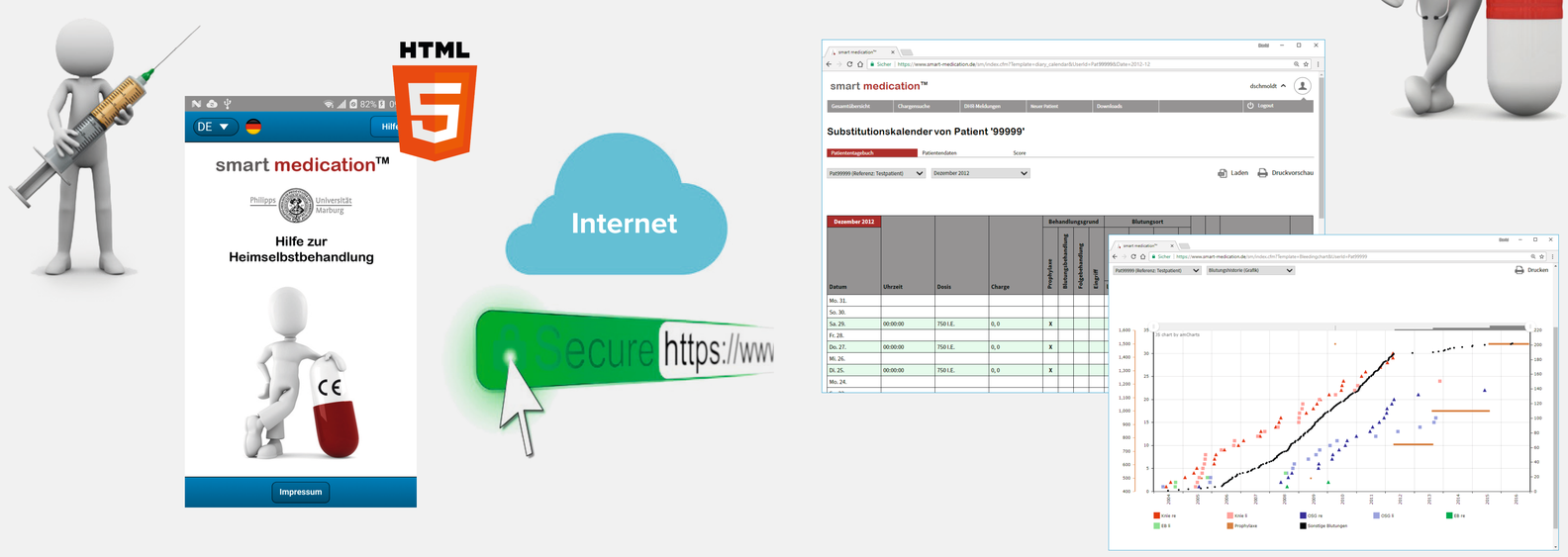


Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

Health-specific implementation guidance
In addition to the guidance given by ISO/IEC 27002, guidance on policy for the issuance and use of digital certificates in healthcare and on the management of keys can be found in ISO 17090-3

FIG. 1 APPLICATION OF CONTROL **10.1.1 POLICY ON THE USE OF CRYPTOGRAPHIC** AND **9.2.1 USER REGISTRATION AND DE-REGISTRATION** IN SMART MEDICATION™

Proper and effective use of Access Control and Cryptography within smart medication™ :
- end-to-end encryption of communication btw. patient and doctor
- pseudonymization of patient id (no use of name, address, etc.)
- no app distribution via commercial app stores (due to HTML5 app provisioning)
- maximum protection of users privacy (no data to be disclosed to any third party!)



Results:
It is shown how security controls and principles defined in the ISO/IEC 27001 and 27799 series are applied to the smart medicatio™ 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.

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.