Certifications	Definition
C5	**Secure cloud computing standards.** The C5 (Cloud Computing Compliance Criteria Catalogue) criteria catalogue specifies minimum requirements for secure cloud computing and is primarily intended for professional cloud providers, their auditors and customers. It is the foundation for putting a customer-specific system of risk management in place. The C5 criteria catalogue was first published by the Federal Office for Information Security in 2016 and has since established itself successfully on the market. According to the BSI, over a dozen attestations have already been granted for national, European and global cloud providers, as well as a wide range of cloud services. Medium-sized and small providers now use the catalogue too.
HDS	**Trust and compliance in eHealth data hosting.** The HDS certification (*hébergeur de données de santé* in French) is a designation that signifies a trusted environment built around eHealth and patient monitoring. Its primary aim is to strengthen the protection of personal health data. This certification is based on frameworks that are in compliance with ISO standards, allowing an accredited independent body to certify any structure or organization hosting health data.
ISO/IEC 27001	**International standard for information security.** ISO/IEC 27001 sets out the specifications for an effective ISMS (information security management system). It helps organisations manage their information security by addressing people, processes and technology. Certification to the ISO/IEC 27001 standard is recognized worldwide to indicate that Doctolib's ISMS is aligned with information security best practices.
ISO/IEC 27701	**Privacy management for personal data in ISMS.** ISO/IEC 27701 is a privacy extension to ISO/IEC 27001. The design goal is to enhance the existing Information Security Management System (ISMS) with additional requirements in order to establish, implement, maintain, and continually improve a Privacy Information Management System (PIMS). The standard outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage privacy controls to reduce the risk to the privacy rights of individuals.
ISO/IEC 27017	**Information Technology / Security / Information security for Cloud services** ISO/IEC 27017 gives guidelines for information security controls applicable to the provision and use of cloud services by providing: - additional implementation guidance for relevant controls specified in ISO/IEC 27002; - additional controls with implementation guidance that specifically relate to cloud services. This Recommendation | International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers.
ISO/IEC 27018	**Information Technology / Security / PII in Cloud** This certification aims to establish commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. In particular, this document specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which can be applicable within the context of the information security risk environment (s) of a provider of public cloud services. This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which provide information processing services as PII processors via cloud computing under contract to other organizations. The guidelines in this document can also be relevant to organizations acting as PII controllers. However, PII controllers can be subject to additional PII protection legislation, regulations and obligations, not applying to PII processors. This document is not intended to cover such additional obligations.
TÜV geprüfter Datenschutz v5.0	**System compliance and documentation check.** It signifies that a company or website has been audited and meets specific criteria regarding data protection and privacy according to German standards.
TÜViT Videosprechstunde	**IT security and compliance for video consultations.** For patients to be able to use video consultations safely and ensure the data protection-compliant processing of patient data, the legislator has tasked the National Association of Statutory Health Insurance Physicians (KBV) and the National Association of Statutory Health Insurance Funds (GKV-Spitzenverband) with defining the necessary technical requirements. Providers of video consultation solutions must provide evidence of data protection and information technology security of their service to be listed as certified video service providers. TÜVITs "Trusted Site Video Consultation (TSVC)" testing and certification procedure provides the required evidence of the information technology security of video consultation solutions. As part of the certification, the IT security experts review the relevant IT infrastructure of video service for compliance with the "Regulations on Information Technology Security" according to Annex 31b of the Federal Contract Physicians (BMV-Ä). The procedure TÜVIT has developed is approved by the German Accreditation Body (DAkkS).
TÜViT Datenschutz	**GDPR video consultation services compliance.** TÜVIT also pursues certification according to Article 42 of the GDPR for the technical provision of video services to doctors to conduct video consultations per Section 365 (1) of the German Social Security Code (SGB V) in the field of data protection.
NEN 7510	**Health informatics - Information security management in healthcare - Part 1: Management system** Organizations in the Netherlands that process patient health information must demonstrate control over that data and their organization consistent with the requirements set out in the NEN 7510 standard.

Last update: 2024-01-17