MYRA

WHITEPAPER

IT security creates the foundation of trust for e-health solutions

IT security creates the foundation of trust for e-health solutions

Patients in Germany are witnessing a fundamental change to their healthcare system. New digital solutions, such as the electronic patient record (ePA), the e-prescription, electronic certificates documenting incapacity to work (eAU), or the recently adopted digital vaccination certificate, are increasingly replacing their analog equivalents.

Detailed information on examinations, diagnoses, therapeutic measures, treatment reports, vaccinations and medication plans are electronically generated, archived and communicated. The smartphone is developing into a centralized health hub providing an interface that can be used to reach doctors, health insurance companies and hospitals. This far-reaching transformation is enabling immense increases in efficiency. Critical health data is available at all times, allowing unnecessary multiple diagnoses and examinations to be avoided when a patient changes doctor practices.

> *We can only improve patient care if we take advantage of the opportunities afforded by modern digital technologies.*
>
> Former Federal Minister of Health
> Jens Spahn on the importance of digital processes in healthcare – WiWo, April 12, 2019

E-health: the critical significance of web portals

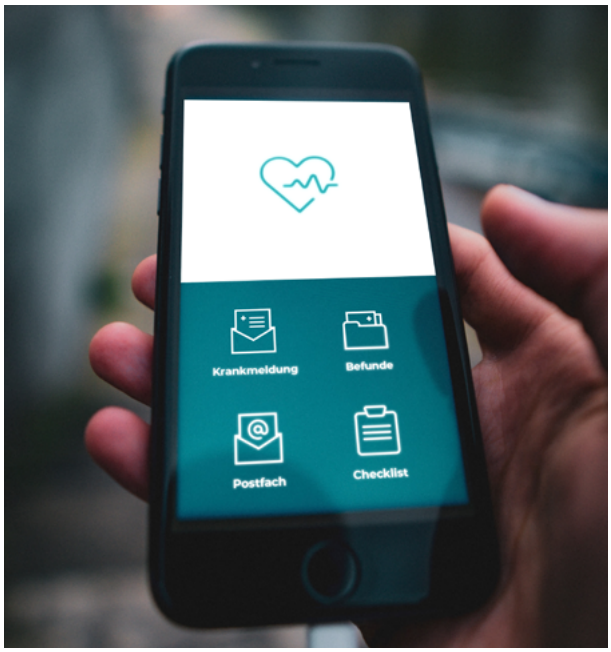
Online services form part of the everyday life of a large part of the population. Web services, such as for mailing, office tasks, and media streaming, have made huge advances in recent years, and they are now in no way inferior to the classic programs and apps for PCs, tablets and smartphones.

Patients also expect the same level of performance and stability from new online health portals. If there are performance-related delays or failures, this casts a bad light on the underlying technology. Even if sensitive data is not endangered per se, a stuttering web presence is enough to significantly weaken the trust patients will have in an e-health solution.

For this reason, performance and stability must be ensured, especially in cases where patients will be using the solution. Doctors and hospital staff also expect the same level of technical sophistication. The technology should make the everyday life of professionals easier and not add any additional complexity.

Therefore, in order for doctor practices to take full advantage of innovative digital technologies, their patients must first accept the solutions themselves. For this to happen, the technologies must offer concrete added value and, above all, win over the trust in the technology. The German Federal Ministry of Health (BMG) wants to foster this trust by imposing strict data protection requirements.

The protection of critical patient data is one of the guiding principles of all digital medical solutions. That, in turn, requires IT security at the highest level. For this reason, the German Hospital Future Act (KHZG) ties funding for hospitals to investments in IT security.



Diagnoses, therapy measures, medication charts and much more can be managed with mobile ePA using a smartphone app. For the e-health solution to be a success, it must have excellent security, data protection and performance.

Coping with demand and external attacks: Challenges for digital infrastructure

Comprehensive e-health solutions, such as ePA and the digital vaccination certificate, are designed to be used by millions of citizens. The online portals and interfaces for these services must therefore be able to work without flawlessly, even during unanticipated traffic peaks.

In 2020, the corona pandemic showed just how much critical services must be quickly and flexibly scaled. Especially during the spring, the official information portals of government health agencies had to cope with traffic that was up to 100 times greater than normal. Services without sufficient server capacity or protection from becoming overloaded by excessive traffic are inevitably brought to their knees in these situations.

Possible consequences of cyber attacks on e-health solutions and telematics:

- Delayed transfer of critical emergency data
- Difficulty prescribing medication in emergency situations
- Superfluous multiple examinations
- Delayed treatment
- Patients do not have access to their own health data
- Fines for data breaches & data leaks

Heavily used infrastructure is also the preferred target of choice for external attackers. If systems are already strained to their limits, even minor negative external impacts are enough to bring a system down. Cybercriminals can perpetrate such attacks with limited strain on their own resources and still provoke serious failures. Cyber incidents are therefore currently considered by the Allianz financial services company to pose the greatest risk to the healthcare system, right up there along with pandemic outbreaks (Allianz Risk Barometer – Results Appendix 2022).

But IT infrastructure with sufficient reserves is also increasingly at risk of external attacks. Since the beginning of the corona pandemic, the healthcare system and other critical sectors have increasingly come under attack. Cybercriminals targeting vital services are motivated by either financial gain or for political reasons. This is shown by both the mitigation data from Myra and studies by Interpol, the German Federal Criminal Police Office (BKA) and the German Federal Office for Information Security (BSI).

Data protection hurdles when choosing a service provider

According to Article 9 of the General Data Protection Regulation (GDPR), health data is considered to be particularly sensitive and therefore requires correspondingly stringent protective measures, including also information on vaccinations and vaccination appointments. The high demands that are placed on IT security for e-health solutions are also reflected in the regulatory requirements of the German Federal Ministry of Health (BMG) and gematik, the German health IT agency, which are becoming increasingly more demanding. This trend will continue and critical infrastructure (“KRITIS”) in particular must take heed of these requirements. E-health operators, hospitals and doctors will therefore have to address internal data architecture and compliance-relevant issues much more intensively. Supporting information on how to implement this infrastructure is detailed in the industry-specific B3S standard.

Outsourcing IT security needs is an efficient alternative to managing costly in-house operations. Managed service providers handle the implementation, maintenance and operation of the required security solutions, thereby freeing up valuable resources that can be devoted to the core business. By following this strategy, companies can avoid additional expenses for software, hardware and personnel. Due to a competitive job market, highly qualified IT specialists are difficult to find in any case. As of the end of 2019, more than 100,000 positions in this field remained unfilled nationwide.

Of course, it is important to carefully select a service provider. With the expiration of the Privacy Shield Agreement governing the transatlantic transfer of data between Europe and the USA, cooperation with US providers is on shaky ground because there is no legal basis. Data protection regulations are difficult to implement due to the conflicting positions of European GDPR and US law. Such hurdles can be avoided by choosing local providers who are subject to the same jurisdiction and meet the highest data protection requirements.

What makes Myra the right partner for e-health

- GDPR-compliant specialist provider with relevant industry expertise (health, vaccination platforms, federal government, ministries, learning platforms, critical infrastructure, finance)
- Service provided at German data centers
- Myra fulfills all 37 performance requirements of the BSI [German Federral Office for Informations Security] for qualified DDoS protection providers.
- Security Operations Center: 24/7 full-service support from our IT experts
- ISO 27001 on the basis of IT-Grundschutz (IT baseline protection): Certified DC locations & institution
- BSI-KRITIS certified, PCI-DSS certified, trusted-cloud certified, BSI C5 in preparation

Myra is the specialist provider for the healthcare sector

Myra Security develops and operates highly certified protection solutions to secure digital business processes. As a specialist provider for sensitive and critical infrastructure, we have many years of experience protecting companies and organizations in the healthcare, finance and insurance industries as well as in the critical infrastructure and government sectors. Customers in these highly regulated areas benefit from certified security and compliance with GDPR, IT-SiG, BSI-KRITIS and industry-specific standards.

Myra secures the online portals of government agencies such as Infektionsschutz.de belonging to the German Federal Centre for Health Education (BZgA) and the web portal of the German Federal Ministry of Health (BMG). Myra also protects the vaccination portal of the Association of Statutory Health Insurance Physicians for the North Rhine (KVNO) from attacks and excessive traffic. Since they play a central role in fighting pandemics, protecting such institutions should be a top priority.

Certified by the German Federal Office for Information Security (BSI) in accordance with ISO 27001 on the basis of IT-Grundschutz (IT baseline protection) | Certified in accordance with the Payment Card Industry Data Security Standard | KRITIS certified in accordance with Section 3 Act to Strengthen the Security of Federal Information Technology (BSI-Gesetz) | Compliant with (EU) 2016/679 General Data Protection Regulation | C5 certified by the German Federal Office for Information Security (BSI) | Tenants Attested Trusted Cloud Service | IDW PS 951 Typ 2 (ISAE 3402) certified service provider |

Myra Security is the new benchmark for global IT security

Myra technology monitors, analyzes and filters malicious internet traffic before virtual attacks can do any real harm. Our certified Security-as-a-Service platform protects your digital business processes from a wide range of risks, such as DDoS attacks, bot networks and attacks on databases.