GUIDELINE

DIGITIZATION AND PATIENT SAFETY
Risk Management in Patient Care

AKTIONSBÜNDNIS PATIENTENSICHERHEIT

patientensicherheit schweiz

Plattform Patientensicherheit

Inhalt

Foreword by the President of the Federal Office for Information Security (BSI)

Arne Schönbohm
President of the Federal Office for Information Security (BSI)

We are living in a time of rapidly advancing digitisation in all areas of daily life. Progress in this area is being driven by innovative entrepreneurial ideas, a desire to improve efficiency and many positive personal experiences with information technology across a range of fields.

There has never been a society with a higher level of technological affinity across all generations. Digitisation is encountering a market environment that is eager to be thrilled by new technology.

Progress is always associated with learning to cope with new challenges and threats. New technologies are accompanied by new risks. Rejecting new technology or ignoring the risks are not viable alternatives. Instead, an open and sustainable approach to innovation is required. We need progress to secure our future, but this can only be achieved successfully if we are capable of analysing and managing emerging risks.

Especially when extremely sensitive data is being stored and processed, IT security measures need to be in place and must not be sacrificed for greater comfort and efficiency. In order to effectively counter the threats posed by digitisation, we need increased levels of awareness and IT-competencies across the board. Successful digitisation is not possible without information security! This especially applies to the healthcare sector.

One of the consequences of digitisation is that physical borders or spatial distances are no longer sufficient to protect the interests of the individual.

Within the medical care sector, it is therefore vital to implement enhanced risk management procedures that go beyond established approaches from the field of medical devices. Networked patient care requires security measures that go beyond physical solutions and extend not only to surgeries, but also to the devices and data in the patients' hands. Such measures are often difficult to establish when they are new to those affected and cause additional effort on the part of the operator that can negate the actual gain in comfort of the new technology.

There is significant potential for further digitisation in medicine and the speed of innovation is high.

As Germany's national cyber security authority, the BSI shapes information security in digitisation through prevention, detection and reaction, thus facilitating modern and secure lifestyles for all citizens. The BSI views the recommendations in this brochure as an expedient way to increase the awareness and competencies of all stakeholders involved in medical care. Through the use of scenarios, the recommendations manage to bridge the gap between real world patient care, especially in surgeries, and the abstract world of patient data, thus creating a link between enthusiasm for technology and professional responsibility. This will markedly increase the level of IT security in medical care and create the necessary preconditions for all of us to benefit from the advantages of successful digitisation in the healthcare sector.

Editors' foreword

Hedwig François-Kettner
German Coalition for Patient Safety (Aktionsbündnis Patientensicherheit e.V., APS)

Dr. Brigitte Ettl
Austrian Network for Patient Safety (Plattform Patientensicherheit Österreich)

Prof. Dieter Conen
Swiss Patient Safety Foundation (Stiftung Patientensicherheit Schweiz)

Digitization is now commonplace in almost all areas of everyday life and is already an integral part of healthcare. New digital technologies and applications are opening up new opportunities in medicine to make healthcare even more effective and efficient. However, spectacular cases have highlighted the risks associated with digital technology as part of the healthcare system. These include direct harm not only to the performance of healthcare systems, but also to patient safety in terms of physical and psychological safety as well as social inviolability.

The organizations for patient safety in Germany, Austria and Switzerland receive a large number of inquiries regarding digitization. The changes brought about by digitization are dynamic, comprehensive and in some cases their consequences can be disruptive. In order to do justice to these developments, it is necessary to work together. Furthermore, significant challenges associated with digitization do not end with national borders. The German Coalition for Patient Safety (Aktionsbündnis Patientensicherheit (APS)), Austrian Network for Patient Safety (Plattform Patientensicherheit Österreich) and Swiss Patient Safety Foundation (Stiftung Patientensicherheit Schweiz) are now pleased to present two collaborative publications containing recommendations for digitization and patient safety. The first publication addresses patients and makes

recommendations for the safe use of health apps (www.aps-ev.de/patienten-information/). The publication presented here outlines some of the challenges and opportunities that digitization poses for risk management.

Due to the increasing spread of digitization, the nature of the risks relevant to patient safety is changing. While some risks can be minimized, new ones arise and others are growing substantially.

These recommendations are intended for members of all occupational groups who are active in all areas of medical specialization within the healthcare system. The aim is to:

Increase awareness of the new or growing risks associated with the digitization of the healthcare sector.

Inform about possible cause-effect relationships inherent in these risks in order to facilitate an understanding of these seemingly abstract concepts.

Assist in conducting a risk-benefits assessment for existing and planned digital innovations in order to minimize existing or potential risks and to capitalize on the opportunities offered by these new technologies in a way that benefits all stakeholders.

Effective risk management focuses on a small number of highly relevant risks in accordance with the phrase "Less is more!" Therefore, we restrict our recommendations to what we consider to be six of the most significant risks to patient care arising from the use of digital technologies and systems. We are not attempting to produce an exhaustive catalogue, but to facilitate a systematic, meaningful initial engagement with the topic.

These recommendations are not intended to replace consultations with IT specialists nor individual, customized risk assessments that consider the specific situation on-site. In some cases, additional risks to the ones treated here may be of great significance to patient safety. Although preventive measures can minimize a risk, it will never be possible to achieve a completely risk-free implementation of digital systems.

In order to arrive at the recommendations, a modified form of the scenario analysis described in the Technical Rule ONR 49002-2:2014 was used. This procedure facilitates complexity reduction by schematically representing a situation, thus making it easy to understand for everyone involved. Tangible, practical examples were developed to clarify the circumstances of each scenario that arose. These specific examples can basically be applied to all sectors and medical specializations, even if not all risks are equally salient across all fields.

Focusing on the risks posed by digitization in the healthcare system reveals not only the indisputable wealth of opportunities, but also the inherent serious risks to patient safety. Therefore, as is the case with pharmaceuticals and medical products, digital applications for healthcare should be subjected to a risk analysis and appropriate evaluation so as to best realize the opportunities presented by digitization in the sense of good and safe patient care while, at the same time, minimizing associated risks.

Before going to press, these recommendations were read and commented on by numerous experts and practitioners representing various fields. We would like to thank all those who contributed valuable comments and our special thanks go to all the members of the working group.

Digitization and Patient Safety – How well prepared are you?

The following questions highlight central aspects of the risks associated with increasing digitization:

How can you ensure that in the event of an outage or malfunction of IT infrastructure the treatment of patients can continue safely?

Which measures do you employ to guarantee safe patient care when using digital, network-connected medical devices?

Are your IT networks and the network-connected medical devices you employ sufficiently protected against manipulation and data theft by means of external attack?

Are your digital data sufficiently protected against unauthorized access by third parties (e.g. inquisitive relatives)?

If you entrust external service providers with data, which measures do you employ to protect yourself against data loss or abuse?

Do all responsible staff have sufficient digital literacy to recognize malfunctions and weak spots in the IT system affecting the safe treatment of patients?

Digitization and Patient Safety – The Key Issues

In summary, the following basic recommendations were arrived at based on the six prioritized risks.

1. As management, assume responsibility for digital security.

2. Name a Safety Officer for your IT system and network-connected medical devices, and define safety levels.

3. Ensure sufficient resources in terms of time, personnel and materials to guarantee long-term infrastructure security, also with regard to IT security knowledge among staff.

4. Make sure that everyone involved has the necessary knowledge about the risks associated with digital interfaces, passwords and data carriers. Ensure that passwords conform to current security standards and are changed regularly.

5. Ensure that all staff are aware of the risks of digital applications and of practical measures to prevent unauthorized access (e.g. hiding data from view).

6. Provide the spatial environment that facilitates a secure digital workplace.

7. Regularly conduct individual risk analyses to determine which malfunction or outage of which IT system has what impact on patient treatment. On this basis, develop a contingency plan for IT systems and network-connected medical devices including measures to be taken and information to be given.

8. Regularly remind higher level management of the necessity for a contingency plan for IT systems and network-connected medical devices as part of emergency and crisis management procedures. Provide appropriate training for the staff who could be affected so that in the event of an emergency, theoretical knowledge can be implemented effectively in practice.

9. Make sure that the redundant systems and services that are necessary to maintain care standards in the event of IT and/or network-connected medical device outages are permanently available.

10. Only entrust data to external service providers if they can prove that they comply with the legal requirements (European General Data Protection Regulation).

11. Contractually agree contingency plans with external providers and explain liability issues.

12. Determine whether the infrastructure of the external provider is compatible with your hardware and software.

13. Ensure that hardware and software are compatible, validated and calibrated, especially after the replacement of individual components and the expansion or update of a system.

14. Pay attention to the compatibility of the security and performance requirements of IT systems and network-connected medical devices and adapt them after new purchases.

Digitization and Patient Safety – Risks relevant to Patient Safety

Based on a multilevel, partially blinded consensus process the authors identified six key risks relating to the impact of digitization on patient safety. These are presented below.

Risk: ▶ Inadequate protection of the IT network against external attacks

INTRODUCTION

Electronic connections facilitating communication within healthcare teams or with patients are at risk of deliberate "attacks" by criminals. Individuals break into IT networks for a variety of reasons, for instance in order to intercept sensitive data, to delete or manipulate data or to prevent access until a ransom is paid.

PRACTICAL EXAMPLES

Staff in a hospital receive faked phishing emails, supposedly from the IT Department. The email informs them of a new application and requests that the recipients follow a link in order to check whether they can access the system in question. The recipients are instructed to use their user name and password from their user profile for the log in. The link leads to an external site with the hospital's logo. The data entered there are captured and used for an attack on the IT system.

Mr M. has gained access to a treatment room in a psychotherapy practice by faking psychosomatic symptoms. Since there are more urgent cases to be tended to, the "patient" has been left alone in the room to wait for treatment. Mr M. connects his smart phone with a USB cable to the easily accessible practice computer and downloads the patient database. Using these data, Mr M. blackmails both the psychotherapists who run the practice and their patients.

BACKGROUND

The possible avenues leading to an attack on an IT system are diverse and complex. Software, for instance, can often be vulnerable, especially if not updated re-

gularly and not protected by a firewall. Hackers can exploit known vulnerabilities to gain entry to IT systems and install computer viruses.

Data can also enter the system via an external interface, for example on a data CD containing test results. Furthermore, data from apps or information stored on data carriers like USB flash drives can introduce malware into a closed software system in a practice.

Email attachments containing malware or faked phishing emails can prompt users to install malware. If data are transferred without encryption, third parties can intercept and capture sensitive data. If administrator rights are unprotected and available to all, there are no controls over which software can be downloaded and installed.

Networks require interfaces that facilitate linkages between programs. When a large network is attacked or system outages occur, ensuing damage to data may not be limited to one software module (e.g. that of the laboratory or the X-ray department), but can spread through the whole network (domino effect).

There are many motives for using malware (e.g. ignorance, blackmail, destruction, information theft/espionage). Cybercrime in the healthcare sector is already causing significant economic harm and is often highly lucrative for criminals.

Blackmail attempts involving small amounts of money are often successful, because cyberattacks in the healthcare sector lead to high levels of stress and fear for the reputation of the organization in questions. In a similar vein, organizations are reluctant to report attacks to the official authorities based on misplaced shame and reputation-related anxiety, thus allowing cybercrime to spread more easily.

RISKS

- Sensitive data on patients are not protected and can be spread to people outside the organization (data protection).
- The system can cease to function, for instance due to a virus that causes buffer overflow, which interrupts the processes within the organization and may endanger the provision of care.
- Existing data can be encrypted. Criminals use this method to blackmail organizations and to disrupt workflow.
- Data (e.g. laboratory reports, medications, etc.) can be manipulated, thus directly endangering patients.

IMPACT

- If data relevant to patients falls into the hands of an unauthorized third party, they can use this information to disadvantage, stigmatize or otherwise infringe on the privacy rights of these patients at their workplace, in their private life or when they try to enter into contracts or insurance policies.
- Malware can reduce the accessibility of data relevant for the treatment of patients (see Risk: Non-availability of IT infrastructure/patient data).
- Manipulated data can lead to errors of judgement, false diagnoses and consequently to adverse events. Furthermore, the functioning of medical devices can also be affected (e.g. turning off an alarm system).

POSSIBLE CAUSES

- Insufficient risk awareness due to limited digital literacy (see Risk: Insufficient digital literacy within healthcare teams).
- Lack of IT network security comprising firewall, virus protection and quarantine for emails can make it possible for external third parties to infiltrate the network with little effort.
- Viruses can make unencrypted emails legible for third parties. This allows information and data to be stolen easily.
- Possible entry ports for malware are, for example, non-secured USB ports on PCs or unencrypted Wi-Fi networks. USB flash drives containing viruses may also be distributed intentionally.
- Medical devices are often connected to IT networks. A member of staff servicing a medical device can inadvertently allow a virus on a USB flash drive to enter the medical device and from there the IT network (see Risk: Insecure integration of active medical devices into IT networks).

RECOMMENDATIONS FOR MINIMIZING RISK

- Regular data protection training for staff that refers to the importance of password protection (simply facilitating unauthorized access to data contravenes data protection guidelines).
- Every network requires authorized staff responsible for network administration. Access must be limited and protected with special passwords and security levels.

- Regularly update software and firewalls to keep the security barriers for your IT network up to date.
- Lock entry ports (e.g. USB ports) on computers in the workplace. Storage media should first be checked for viruses on a secure PC.
- Use additional anti-virus software to secure the connections between medical devices and the IT network and lock external entry ports on medical devices and only unlock them after external storage media have been checked for viruses.
- Do not cover up attacks or damage inflicted by third parties but report it so that others can learn from the experience and react promptly (reporting system).

Risk: ▶ Insufficient protection of the IT network against unauthorized access

INTRODUCTION

In practices or hospitals it can often happen that third parties unintentionally gain access to sensitive information. This commonly occurs when conversations between staff members are overheard by patients (e.g. in lifts or canteens). Increasingly, however, unintentional data breaches are taking place due to poorly secured IT structures.

PRACTICAL EXAMPLE

In a GP's practice, patient data are stored on one central PC which serves as an information source. Patients can view the monitors from the side. No screen savers have been installed, so visitors can read the screens. A waiting patient happens to see the name of a colleague who frequently misses days at work for health reasons. The patient informs his other co-workers of the valid reason for the colleague's time off.

BACKGROUND

Passwords and screen savers that prevent viewing of open files are often not installed on PCs. PCs in treatment rooms can often be accessed without a password. If waiting rooms and treatment rooms are not physically separated, patients may spend a long time unsupervised in treatment rooms. Prolonged waiting times, curiosity, boredom, a desire for information about other patients/relatives/third parties (e.g. emergency services) can lead individuals to seek unauthorized access. In order to save space, PC monitors are often positioned in patients' direct line of sight, thus allowing them to view the information onscreen. An inadequate physical separation of PC-workstations from the general public (e.g. a ward trolley standing in a corridor) can facilitate access to sensitive data by unauthorized third parties.

RISKS

- Sensitive patient data are not protected and can be spread to external individuals (data protection).
- Data (e.g. treatment plans) can be manipulated and can thus directly endanger patient safety.

IMPACT

If data related to patients falls into the hands of an unauthorized third party, they can use this information to disadvantage, stigmatize or otherwise infringe on the privacy rights of these patients at their workplace, in their private life or when they try to enter into contracts or insurance policies.

POSSIBLE CAUSES

- Lack of time is frequently mentioned as a cause. The need to repeatedly log on is perceived as time consuming and impractical.
- Frequently changing staff (e.g. shift changes, part-timers) means that not everyone has their own user account. To ensure that all staff still have access, passwords are often not required.
- Levels of awareness or compliance may not be sufficient among staff. They may not be fully aware of the consequences of negligent IT security.

RECOMMENDATIONS FOR MINIMIZING RISKS

- Regular data protection training for staff that refers to the importance of password protection (simply facilitating unauthorized access to data contravenes data protection guidelines).
- Correct setup of computer workstations in public areas, for example using privacy filters for monitors.
- Using special access codes to protect certain functions of the IT network in order to minimize the number of individuals with access to patient data.
- Using passwords to secure IT networks. However, passwords are only helpful if they are regularly updated and not written down next to the workstation.
- Using transponder systems/biometric data profiles to encrypt IT networks. This would secure the workstations and also ensure rapid access to networks.

Risk: Non-availability of IT infrastructure/patient data

INTRODUCTION

IT infrastructure allows for a rapid and comprehensive exchange of patient care data and also reduces the physical space required for archives, thus facilitating more effective and faster treatment. Electronic patient files and digitally available images can be viewed simultaneously in different places, while creating backups can contribute to improved data security.

PRACTICAL EXAMPLE

Due to the outage of a server in a healthcare centre, it is not possible to access patient data. Furthermore, new test results cannot be saved in the patients' files. Without access to patient data, more complex medical treatments may not be possible. The remaining possibilities for treatment are recorded on paper to be entered later into the patients' digital files. The functionality of the entire healthcare centre is reduced to a minimum and most appointments are cancelled because the digital appointment system is also inaccessible. Queries from the emergency department of the local hospital regarding the anamnesis of a patient previously treated at the healthcare centre can only be answered partially. It takes hours to reach the IT company responsible for the server and the earliest repair date they can offer is two weeks away, since the type of server that could be configured for use at the healthcare centre would not be available earlier. When asked about contingency plans for IT outages, both the general manager and the staff look perplexed.

BACKGROUND

All the sectors and professions involved in patient care are becoming ever more dependent on IT infrastructure. In many facilities anamneses are recorded digitally and diagnostic investigations such as imaging are not only conducted using IT systems, but the results are also sent, allocated to the correct patient and stored in a retrievable form by digital means. Similarly, therapeutic procedures are increasingly being electronically documented and IT systems are also being used to pass on information, for instance referral letters or prescriptions, to other actors involved in the care of the patient. Under normal circumstances, this requires fewer resources than a purely paper-based documentation and can improve data

quality (e.g. better legibility of prescriptions). However, when the IT infrastructure fails, diagnostic and therapeutic options for treating patients may become unavailable on the one hand and, on the other hand, it may no longer be possible to access previously recorded patient data. System malfunctions may be bridged by the implementation of paper-based procedures for treatment documentation, which can be differently organized across different contexts. Depending on the extent and duration of the malfunction, this can facilitate continued treatment with limited adverse consequences for the patient. While certain elective treatments can be postponed until the IT system is up and running again, the loss of information, especially concerning essential treatments, is an enormous safety risk. Previously compiled essential patient information cannot be accessed (e.g. previous illnesses, medication history including known allergies or adverse reactions). If the patient is critically ill, frail and/or polymorbid it is not always possible to obtain the necessary information from them. Consequently, treatments that may seem necessary in the moment may in fact counteract previously established treatment. Similarly, the loss of IT-based diagnostic and therapeutic instruments is associated with serious risks for patients in acute need of treatment who may have to be moved to another health service provider.

RISKS

- Impaired or lost functionality of diagnostic and therapeutic instruments.
- Inability to access or pass on existing relevant health-related information.
- Loss of instructions for organizational procedures.
- Limitation or severe delay in internal and external communication.
- Potential loss of information in the process of transferring offline documentation to the IT system once it has been repaired (loss of information).

IMPACT

The loss of certain diagnostic and therapeutic options and/or access to relevant health-related information can lead to a delay in implementing the treatment. Especially patients in acute need of treatment may then suffer harm, for instance due to

- The interaction between new medication and previously prescribed (but now unknown) medication;
- A break in the continuity of care through involuntary cessation of the previous therapy or inadequate monitoring of the therapy;

- Malfunction of therapeutic systems during an intervention;
- Unnecessary exposure to emissions due to repeated examinations;
- The need for transfer/referral to an external healthcare provider;
- Errors in manual post-hoc documentation after functionality of the IT system has been restored.

Compensatory measures, up to and including personal individual monitoring of patients if monitoring equipment fails, require staff to commit all possible skills and resources to the exceptional situation. Further harm may ensue from this acute strain on staff by increasing the likelihood of errors. Outages at the start of the treatment chain can have a knock-on effect on treatments further down the line. The organization's performance capabilities are severely limited and may cease entirely in some areas; the damage to the organization's reputation may be considerable.

POSSIBLE CAUSES

- Insufficient awareness of contingency plans and necessary redundancies, especially in supposedly "non-critical" areas outside of emergency care.
- High pressure to innovate without sufficient validation and testing before implementing new elements within the increasingly complex overall IT system.
- Lack of contingency plans to rapidly alleviate IT system failures.
- Lack of training and awareness of affected staff about how to behave during an IT outage so as to prevent documentation errors.
- Insufficient staff and material resources to protect the IT system from malfunction and failure.
- Absence of redundant systems (pre-configured substitute systems).

RECOMMENDATIONS FOR MINIMIZING RISKS

- Sensitizing higher level management to the need for individual contingency plans (Service Level Agreements) and redundancies based on an individual risk analysis of existing IT infrastructure and considering the organization's operational field.
- Conducting specific risk analyses to estimate the impact of various IT failure

scenarios and deriving individual preventative measures before purchasing a given device.

- Drawing up contingency plans to ensure care provision in the worst case, for instance by deploying more staff, using analogue procedures (e.g. paper and pencil) and developing a crisis communication plan. Firm priorities should guide the preservation of the most important functions and minimize risks to patient safety.
- Providing redundant and compatible systems that are deemed necessary, including supply structures such as communication technology, energy supply, medication supply and waste disposal.
- Separating networks with critical functions (supporting vital functions) from other IT components to minimize their risk of failure if a subsystem malfunctions.
- Including the scenario of IT system failure into existing emergency and crisis plans, in so far as they exist (e.g. hospital emergency response plan, quality management system etc.).
- Appropriate and, if necessary, repeated training for the emergency scenarios so that in the event of an emergency the contingency plan is known and can be implemented. The focus should be on the most important aspects (see Risk: Insufficient digital literacy within healthcare teams).

Risk: ▶ Transferring data to external service providers (e.g. cloud computing)

INTRODUCTION

Cloud computing is a widespread application of digitization in the healthcare sector. When using these IT services, the healthcare providers transfer their data to third parties (cloud computing providers) for processing and storage outside of their direct area of influence. In this way, care providers can rationalize and optimize daily processes as well as offer new services to their patients (e.g. booking appointments online, electronic health files).

PRACTICAL EXAMPLE

A hospital transfers patient data from the operating theatre to an external provider in order to make use of a communication tool designed for use during operations. The tool converts speech to text with the help of a digital assistant. The basic idea is that speech is recorded via a microphone and converted into text by the digital assistant. During this process, the data are analysed and stored on an external computer. The resulting text is either used for the voice control of equipment in the operating theatre (thus improving hygiene because no contact is necessary), or for the direct and immediate documentation of the operation.

Hospital management decides to use the system. After a test period of several months, dictations from the hospital's operating theatres suddenly appear on various hacker forums in the Dark Net. The likelihood of a blackmail attempt or ransomware attack seems high, thus leaving the care provider in a highly vulnerable position. The system is closed down immediately. The subsequent investigation uncovers a bug in the encryption of the data transfer chain between the operating theatre software and the digital assistant. The affected patients intend to bring a class action against the hospital and lasting damage to the hospital's image is also likely.

BACKGROUND

In cloud computing, sensitive data are sent and stored outside of a given organization (hospital, practice). Among the advantages of cloud solutions and outsourcing IT infrastructure are the time and resources saved that can be invested in patient care as well as the nearly universal availability of cloud computing services. Three levels of IT support for organizational optimization are commonly distingu-

ished. Using the cloud fundamentally offers advantages at all levels. These are listed below in ascending order of the level of service offered by the cloud provider:

- **Infrastructure as a service**: only the hardware (server, network) is provided, the user is responsible for maintenance of the operating system and the software.
- **Platform as a service**: in addition to the hardware, the operating system is also maintained.
- **Software as a service**: in addition to the hardware and the operating system, the software itself is also maintained by the cloud provider.

Especially for small organizations or individual professionals, such as general practitioners or psychotherapists in one-person practices, keeping up an entire IT department does not seem cost effective, so outsourcing IT needs to electronic service providers seems attractive. This frees up the professionals to concentrate on their core business. However, in addition to the potential advantages there are also disadvantages.

RISKS

- Data loss: For example, examination results may be lost or no longer available; documentation duties may not be fulfilled; patients may receive redundant diagnostic examinations. In some situations, treatments cannot be carried out on time because the practitioners do not have sufficient information.
- Data abuse: Sensitive and valuable data fall into the "wrong hands". Those holding the data attempt blackmail or to sell them. Publication of the data is a possible consequence.
- Data manipulation: Social engineering (e.g. assuming fake identities – the boss needs the data; harm to the patients, costs).
- If it is not possible to save in the cloud, further actions may be impacted, e.g. archiving the data. The cumulative failures may lead to a system "crash" within hours.

IMPACT

- **Health Impact**. For instance, patient data is not available, so a known sensitivity to certain medication is overlooked. The patient experiences anaphylactic shock and needs intensive care.

- **Social stigmatization and discrimination.** If sensitive patient data become publically widely available, there is a real possibility for individual people or groups to become stigmatized. For example, people with chronic or infectious illnesses may be excluded from the labour market.
- **Costs.** If data are no longer available or have been lost, (possibly invasive) diagnostic procedures may need to be repeated. This may cause additional costs for the care provider and the patient. If the patient is harmed, compensation claims may arise.
- Infringement of **patient autonomy.** Patients are subjected to harm in a non-material sense if their data are processed by external third parties without their knowledge and consent.

POSSIBLE CAUSES

- **Pressure to reduce costs.** Effort is required to guarantee secure utilization of IT systems. Profit-oriented users in competitive environments are under pressure to reduce costs which can lead to a relaxation of necessary standards.
- **Diffusion of responsibility.** Cloud architecture can increase the measure of responsibility attributed to weak links in the communication chain, thus increasing, over time, the likelihood of damages.
- **Inadequate performance.** The cloud computing service may not perform well and its legal basis may be insufficient. Sometimes providers promise more than they can deliver.
- **Sabotage or criminal activity.** By their very nature, healthcare data are sensitive and therefore a potential target for cybercriminals.
- **Environmental impact.** It is also possible that extreme weather conditions, e.g. lightning strikes or flooding, can cause system malfunctions or outages.
- **Economic interests in grey or not yet legalized areas.** Using data collected in the course of day-to-day practice for economic purposes other than patient care without prior approval by an ethics committee.
- **Level of digital literacy among healthcare staff.** The technical and legal implications of externally processing patient data are wide ranging and are not always correctly assessed by healthcare staff (see Risk: Insufficient digital literacy within healthcare teams).

RECOMMENDATIONS FOR MINIMIZING RISKS

- Guarantees. Contractual agreements clearly guaranteeing specified services should be entered into with providers of cloud-based services. It should be noted that the final responsibility for the patients still lies with the medical service provider.
- Standards. Relevant standards and statutory provisions should be observed. Standards for data protection and data ethics should be implemented (Good Practice).
- Reporting. Public documentation of procedures and evidence, for example in quality reports.
- Reversibility of cloud storage. The concept of ePrivacy implies that there should be a reversible "consensus" regarding the storage, usage and further processing of the data that all parties have to agree to. When choosing a provider, it is advisable to select one who can restore local availability of data and who can reverse any action taken in the cloud in terms of storage, processing and transfer.
- Improve digital literacy. Develop the digital health literacy of healthcare teams, organizations but also patients (see the APS Checklist for the use of Health Apps).
- Application and implementation of the European General Data Protection Regulation.

Risk: Insecure integration of active medical devices into IT networks

INTRODUCTION

Medical devices are devices intended for medical use that have been designated to be appropriate for human beings. Medical devices include, for example, X-ray machines and medical instruments, but also medical software. The integration of medical devices into IT networks depends on internal and external influences affecting IT networks and existing software.

Increasingly, apps are being approved as medical devices and they also interact with IT networks (medical apps), see the APS Checklist for the use of Health Apps.

PRACTICAL EXAMPLES

Example 1

To improve practice organization in a healthcare centre, all imaging systems (X-ray, ultrasound, endoscope, operating cameras etc.) are integrated into one network so that the data they generate can be viewed in every treatment room and also by other members of staff (or external practices etc.). During a radiological examination, the image on the monitor freezes. After a restart, all data from the previous examinations have been lost. In spite of a full service contract, the relatively new X-ray machine cannot be restarted because of a virus infection in its outdated operating system. The patient needs to be moved to another facility because the back-up system does not work either. The entire digital infrastructure is affected.

Example 2

A patient dies because the central monitoring system on a hospital ward fails to sound an alarm. Medical personnel were not able to react in time. The system also failed to forward the alarm to a mobile phone as intended.

BACKGROUND

Medical device legislation

Manufacturers of systems for medical technology are tightly bound by regulatory requirements and have to prove the safety of their system in an extensive testing procedure. The tests have to be repeated each time changes are made to the system. This means that it is not possible to react rapidly to threats. Even contracts offer no protection.

Interconnected medical devices

If medical devices and a computer/network form one unit, both are governed by the Law on Medical Devices. Therefore, changes cannot be made to the unit without recourse to the legally mandated procedure. This makes it difficult to undertake routine maintenance (e.g. installing security updates, firewalls, virus scanners etc.).

The increasing complexity of composite IT networks based on the integration of medical devices with clinical networks constitutes a challenge in terms of the special requirements for the IT administration of medical-technical devices and the software for medical devices. At the same time, the integration of medical devices (e.g. for monitoring purposes) can convey a false sense of security and thus also misdirected attention of practitioners.

RISKS

- Interaction and incompatibility between software, hardware and network up to a partial or complete outage of the system.
- Impairment due to external disturbances.

IMPACT

- If the control functions of medical devices are affected, risks to patients range from misdiagnosis to physical harm.
- If errors occur when data are saved, forwarded, evaluated or displayed, these can lead to errors in treatment decisions and/or harm to the patient.

POSSIBLE CAUSES

- Development cycles and certification procedures take substantially longer for medical devices than for other software, which can prevent rapid reactions to threats.
- The manufacturers of medical equipment do not always validate firewalls in real time, which may lead to a lagged reaction to threats.
- A full service contract can lull the operators of medical devices into a false sense of security.
- Service engineers can also contribute to the spread of malware by means of compromised USB flash drives or servicing computers (see Risk: Insufficient protection of the IT network against unauthorized access).

- Due to its short development cycle, software may contain errors (bugs). Devices can malfunction during normal usage and data can be lost if they have to be rebooted.
- Repeated generation of errors and flags can cause control software to crash. These flags can be produced by external outages of the network/Wi-Fi, or they can arise internally from software or component errors.
- Relying too heavily on technology (faith in technology) and underestimating the interactions between medical technology, software and hardware lead to negligence (see risk: Insufficient digital literacy within healthcare teams).
- Integrating short-lived "consumer ware" into medical device combinations or using different software versions in one system.
- External technical influences (thunder storms, electromagnetic interference from other devices, emergency power systems, power fluctuations, mobile phones, private usage of the IT system).

RECOMMENDATIONS FOR MINIMIZING RISKS

- Check all USB flash drives with up-to-date anti-virus software before connecting them to a medical device.
- Plan the maintenance of medical-technical equipment responsibly. Certain preparations are always necessary before outside technicians/firms can conduct their work and should be agreed with them in advance.
- Consider aspects of patient safety when purchasing new medical devices (see APS Recommendations "Improving patient safety by preventing risks associated with medical devices" (Patientensicherheit durch Prävention medizinproduktassoziierter Risiken)). Medical devices with their own operating system may be more secure than those running on common operating systems. When purchasing medical devices, aspects relating to the technical security of existing infrastructure should be part of the specification analysis.
- Strict separation of medical devices from other applications, also within networks, to protect against attacks and hacks (e.g. by means of different, standardized Wi-Fi frequency bands, physically separate alarm network etc.).
- Avoid using short-lived "consumer ware" in combination with medical equipment relevant to security. Instructions regarding intended use as defined by the manufacturer should never be ignored.

- Networks connecting medical equipment should be separated from other networks to avoid mix-ups and address the growing complexity.
- Zoning/segmenting of networks. A complete set of network-connected emergency medical devices can be stored in one zone, a second set of these devices in another, separate zone. If one zone malfunctions or fails, emergency provision can be assured with only a small capacity requirement.
- Consider technology a supportive tool for the user that does not alleviate them of their duty of care and monitoring towards patients and third parties (technology does not replace staff).
- Training and raising awareness among users (see Risk: Insufficient digital literacy within healthcare teams).
- When making repairs or replacements, do not view a medical network as a collection of single components, but as a whole and conduct a risk assessment accordingly (including the risks inherent in networked devices).
- Check the software versions installed and the basic configuration of devices, especially after repairs/replacements (they will often be reset to the factory settings).
- Request a risk analysis from the manufacturer or IT partner to identify potential security gaps.
- Conduct a risk analysis to identify how the device can be protected from damage arising within your own network.
- Change the standard passwords for administrator rights (see Risk: Insufficient protection of the IT network against unauthorized access).
- Invite experts to conduct security audits and security tests to close potential security gaps.
- Adapt emergency plans to the particularities associated with medical networks and update them as necessary (see Risk: Non-availability of IT infrastructure/ patient data).

Risk: ▶ Insufficient digital literacy within he althcare teams

INTRODUCTION

When digital applications are introduced and the use of IT infrastructure is expanded, healthcare teams are often under great time pressure to learn how to use the new applications. During working hours it is often difficult to train all the members of a healthcare team sufficiently (also due to the large number of new applications and the varying levels of familiarity with digital technology) to guarantee the security and optimal implementation of the digital applications. This can mean that the basic rights of patients (e.g. data protection) are endangered or that important digital applications are not adequately protected from external attacks. Insufficient digital literacy, or an overestimation of their extent, can endanger patient safety. If digital products do actually malfunction or are used incorrectly, a crisis management strategy is often absent.

PRACTICAL EXAMPLES

Example 1

The end of the quarter and the holiday period are just around the corner. Patients are waiting impatiently outside the still-locked practice door. The computers are turned on but it takes longer than usual for the system to initialize. Some components cannot be accessed. Later in the morning, another colleague arrives for work and realizes that the virus scanner is switched off. When a patient asks what that means for the protection of her personal data, no one can give her any information.

Example 2

A planned robot-assisted operation looks like it will have to be cancelled because the experienced surgeon who was scheduled to perform it is ill. However, a colleague who considers himself to be digitally competent and who has previously performed this operation offers to take over. During the operation, technical problems arise.

Due to the replacement surgeon's lack of experience with the robot's controlling software and his overestimation of his own digital literacy, the technical problems cannot be solved quickly enough and the patient suffers harm.

BACKGROUND

Limited awareness or knowledge often lead to inadequate protection against unauthorized access and to improper use of information technology. Certain threats to the patient's digital self-determination may only arise as digitization spreads further throughout the healthcare sector and thus cannot be anticipated in advance. Data protection measures and training in digital literacy are perceived as additional work and so trusted routines are maintained. Especially when working under significant time pressure, most attention is directed towards the patient and IT safety aspects may be ignored. However, familiar routines, inaccurate self-assessment by staff as well as out-of-date software and hardware are particularly strongly associated with significant risks. Since risk awareness is often also limited, assuming additional responsibility for IT may be avoided.

Small organizations are often particularly vulnerable to external attacks, since the small number of staff makes specialization or sharing of tasks and competencies harder.

RISKS

- Healthcare teams are not sufficiently capable of informing patients about the risks of digital applications.
- There is a lack of knowledge about the risks of inadequately secured IT infrastructure (e.g. sending sensitive information via email without encryption).
- Limited comprehension of necessary IT security measures often means that "complicated" solutions are preferred over "simple" digital products (overreaction).
- Misjudging the predictive value of systems designed to assist in decision-making (regarding diagnoses/indications).

IMPACT

- Delays in treatment can occur if digital literacy and IT training programmes are insufficient. Such delays can endanger patient safety and even lead to death.
- Misdiagnosis or misinterpretation of the results provided by decision-making support systems.
- Violating the patients' basic rights or their digital self-determination.
- In spite of their benefits for patients, meaningful digital innovations may not be employed.

POSSIBLE CAUSES

- Lack of experience due to the rapid pace of innovation.
- Lack of general risk awareness in relation to digital applications, for instance uncritical handling of emails and attachments.
- Lack of specific awareness of changes in risk types and levels associated with the adoption of innovative technology.
- Carefree routine behaviour: "That's the way we've always done it".
- Individual, unregulated use of software, apps.
- Inappropriate use of social media, e.g. sending patient data on messenger services.
- Mixing professional demands with valued, private tools/devices.
- Lack of password protection or screen savers, insecure interfaces, lack of attention and awareness when using digital applications.
- Intense time pressure with the result that "direct patient care" takes priority over measures to ensure IT security.
- Lack of knowledge about the compatibility of different digital products and systems that can then impact negatively on IT security.

RECOMMENDATIONS FOR MINIMIZING RISKS

Team competence – knowledge provides security at the management level

Actively assume responsibility for the digital literacy of specific teams and the whole organization:

- Safety first – "Not everything that is possible is acceptable. Not everything that is acceptable is also meaningful".
- Regular training, induction of new co-workers, define staff members responsible for providing IT security information.
- Create an internal regulatory framework; communicate it clearly and definitively; keep it up to date.
- Continuously check communication and implementation of IT security measures.
- Seek out literacy in job interviews, during annual reviews and, if necessary, draw up a plan for improving necessary literacy.

Arrange professional IT support:

- Regularly check contracts.
- Secure data storage, efficient data protection – encryption, regulate use of private email accounts, set up mobile devices so that data can be deleted centrally.
- Damage recovery – draw up service level agreements where necessary.

Team competence – knowledge secures the whole organization

Establish concise indicators in the team to help them assess malfunctions and the acute need for action:

- Use simple, reliable alarm systems.
- Whistle-blowers are not disruptors, obstructors or killjoys.
- Correct assessment and communication of acute changes in the system.
- Up-to-date phone numbers that everyone in the team has access to.
- Work according to a code of conduct that is binding for everyone.
- Regular training with the aim of improving digital literacy.
- Awareness of the appropriate procedures for handling digital applications.

Introduce simple, tangible instructions and contingency plans to be followed in the event of malfunctions.

- What is the correct reaction to a critical situation in the IT system?
- Who sets priorities in an emergency?

Self-test for assessing IT security in a health organization

Currently, most devices and most kinds of software are largely comprised of standard components or modules that were not originally developed for use in highly available systems where they have to function constantly and without errors. Consequently, these standard components bring with them a multitude of weak points, undesirable side effects and defects.

While healthcare specialists do not necessarily require detailed knowledge of the types of situations that may constitute threats to IT infrastructure, it is important that they at least gain an overview of the potential danger scenarios that can lead to serious damage. This would allow for an initial assessment of the risks a new system might introduce into a given patient care context. However, it is advisable to consult qualified external IT specialists to ensure appropriate security. If, as a member of a healthcare team, you (intend to) introduce or use a system at your workplace, whether it is a device or an application, it is advisable to first establish the implications of this system for you and your patients. In deciding on whether to use a new system, important aspects include the extent to which your work depends on this system, where it comes from, what technical support is available and the impact a malfunction or outage of the system would have on you, your patients and/or third parties.

A risk matrix can be used to schematically represent the risks as shown below (Fig. 1). In clinical risk management, the credible worst case, which can affect both practitioners and patients severely, should always be considered. While this is less likely than minor routine problems, it is nevertheless useful to conduct a risk analysis for the worst-case scenario.

Risk assessment by means of the risk matrix proceeds with recourse to the dimensions "frequency of occurrence", "likelihood of occurrence" and "impact of the risk" based on pre-defined risk criteria. The following example is based on the risk management regulation ONR 49002-2:2014 and can be used as a guideline for your own risk assessment.

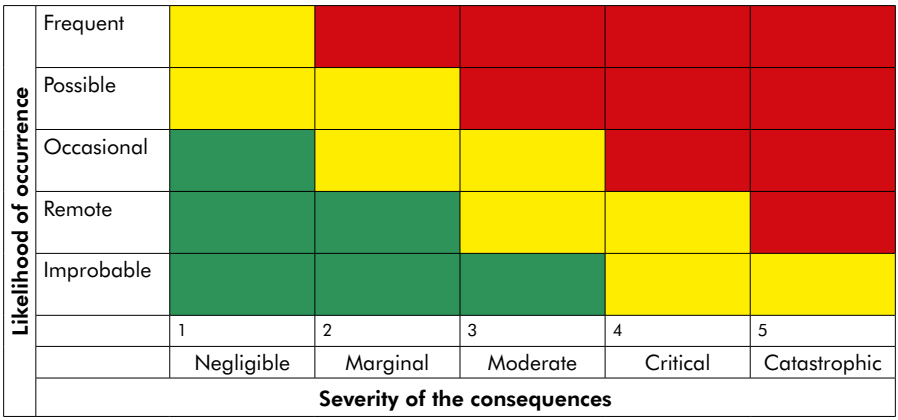

Figure.1: Risk matrix

LEVEL	FREQUENCY
Frequent	Once or more per month
Possible	Once per quarter
Occasional	Once a year
Remote	Once in three years
Improbable	Less than once in 3 years

Frequency of occurrence, Table A3, ONR 49002-2:2014

LEVEL	PATIENT / CO-WORKER	PERFORMANCE
Negligible	Incidents without consequences (critical incident, near miss)	The practitioner's performance remains unaffected
Marginal	Minor health impact with temporary symptoms/ pain, prolonged treatment duration	The practitioner's performance remains unaffected, short-term disruptions to workflow and additional costs arise
Moderate	Major health impact without permanent consequences, significantly longer treatment duration	Temporary reduction of the practitioner's performance, additional costs arise from the treatment and the additional disruption to processes
Critical	Major health impact with permanent consequences. No long-term care needs but reduced work ability	The practitioner's performance is permanently affected. The services on offer are reduced
Catastrophic	Major health impact with permanent consequences requiring long-term care, death of the patient / co-worker	Continuing with the previous range of services is threatened

Impact of the risk, adapted from Table A9, ONR 49002-2:2014

The results of the risk assessment in the risk matrix should be evaluated in terms of their affordability and then prioritized in order to develop appropriate measures in corresponding temporal order.

Checklist for self-testing the IT security of a health organization

1. How essential is the intended system for your work?

- ☐ The system is an addition to my knowledge and skills, i.e. the quality of my work will remain unaffected.
- ☐ The system supports my knowledge and skills, i.e. the quality of my work will be improved by using this system.
- ☐ The system is a necessary precondition for applying my knowledge and skills, i.e. I cannot work (to the professionally required quality) without this system.

2. CE certification, origin, technical support

- ☐ Is the system a CE certified medical device?
  - ☐ If no: Is the IT system being offered by a reliable source?
- ☐ Is qualified (technical) support available to assist you in setting up and operating the system?
- ☐ Is the technical support available during your working hours and can they also assist you outside of these hours (e.g. weekends) in the event of an outage or a malfunction?

3. What would the Impact of a complete system outage or malfunction (caused by IT) be on …

- ☐ the quality of your services and that of your co-workers?
- ☐ the availability of your services and those of your co-workers?
- ☐ the wellbeing of your patients, your own and that of your co-workers?
- ☐ the privacy, availability and integrity of your patient data?
- ☐ the privacy, availability and integrity of your organization's data?

GLOSSARY

Administrator
A person who maintains a computer system or a network (for example an intranet) and has special access rights. (Duden)

App/application
The term "app" is an abbreviation for "application". These are various programs, for example for image editing or sending messages, that run on mobile devices such as smartphones and tablets. They can be downloaded and installed. (Own definition)

Buffer Overflow
If more data than expected are passed to a module via an interface, a "buffer overflow" may result. If the module does not check the length of the transmitted data, the data are written outside the intended area, thus destroying the memory structure (heap or stack). The data can also be coded to manipulate the stack in such a way that the execution of malware code is possible. (BSI)

Bug
Colloquial term for a program or software error that leads to a malfunction of the IT system. (Own definition)

CE certification
The CE certification of medical devices by external "Notified Bodies" confirms that those devices conform to the legal requirements of the European Union. (Own definition)

Cloud/cloud computing
Cloud Computing is understood as offering, using, and billing IT services dynamically adapted to the requirements via a network. Here, these services are only offered and used by means of defined technical interfaces and logs. The range of services offered within cloud computing covers the entire range of information technology, including infrastructure (such as computing power and memory), platforms and software. (BSI)

Computer virus

A computer virus is a non-self-contained program routine that replicates itself to manipulate system areas, other programs or their environment in ways that cannot be controlled by the user. (In addition, the virus might be programmed to cause damage.) (BSI)

Consumer ware

Consumer ware refers to products developed for the private end user that are not compatible with the security requirements necessary for professional use. (Own definition)

Dark Net

The Dark Net refers to networks that are not indexed by search engines such as Google, Yahoo or Bing. These are networks that are only available to a select group of people and not to the general internet public, and only accessible via authorization, specific software and configurations. This includes harmless places such as academic databases and corporate sites, as well as those with shadier subjects such as black markets, fetish communities, and hacking and piracy. (Techopedia)

Fake phishing email

Deceptively real looking emails with a familiar address but from unknown third parties who, by means of social engineering, collect user data for fraudulent illegal activities. (Own definition)

Firewall

A firewall (or security gateway) is a system consisting of software and hardware components for the secure connection of IP networks by means of limiting the technically possible connections to the ones that are formally defined in a security protocol. With regard to network communication, security essentially means that only desired accesses or data streams are permitted between different networks and the transmitted data are controlled. (BSI)

Flag/error flag

Term for a marking in the IT system that indicates a specific status, for example, a system error. (Own definition).

General Data Protection Regulation

European Union regulation on standardizing data protection and privacy of natural persons thus ensuring the free movement of data in the European single market. It came into force on 25 May 2018. (Own definition)

Internet of Things (IoT)

In contrast to "classical" IT systems, the Internet of Things refers to "intelligent" devices that contain additional "smart" features. IoT devices are usually connected to data networks, in many cases wirelessly, and can often access and be accessed via the internet. (BSI)

IT security audit

Systematic process to evaluate an IT system for vulnerabilities and risks with the aim of closing security gaps and therefore minimizing IT security risks. (Own definition)

IT system

IT systems are technical systems for information processing. Typical IT systems are servers, clients, single-user computers, mobile phones, routers, switches, and security gateways. (BSI)

Messenger service

Software that allows the exchange of messages or data of various formats between individual users or user groups. (Own definition)

ON-Rule (ONR)

ON-rules are documents relating to norms produced by the Austrian Standards Institute. During their development phase they do not necessarily meet all the requirements for a full standard. (Austrian Standards).

Ransomware

Ransomware is malware that restricts or prevents access to data and systems and claims to release these resources only upon payment of a ransom. It is an attack on the availability of a security target and constitutes a form of digital extortion. (BSI)

Risk

In the context of clinical risk management, risk is defined as an uncertainty in the provision of patient care that, with a projected likelihood of occurrence

and a projected impact, is capable of causing harm to patients, to the persons involved in their care and/or to the organization itself. (APS 2016)

Risk criteria

Risk criteria are reference points for evaluating the impact of a risk on the organization or on the system. (ONR 49000: 2014)

Risk matrix

A risk matrix is a graphic representation in which risks are classified on a scale according to impact and likelihood and/or frequency. (ONR 49000: 2014)

Service Level Agreement (SLA)

A service level agreement (SLA) is a contract between a service provider (either internal or external) and the end user that defines the quality of service expected from the service provider. An SLA usually includes information on the range of services (e.g., time, extent), availability, reaction time of the provider etc. (Gabler's Wirtschaftslexikon)

Social engineering

In cyberattacks involving social engineering, criminals attempt to mislead their victims into voluntarily disclosing data, bypassing security measures or willingly installing malware on their own systems. In terms of both cybercrime and espionage, the perpetrators are skilful in exploiting perceived human weaknesses such as curiosity or fear to gain access to sensitive data and information. (BSI)

Whistle-blower

A person who provides information on illegal or immoral practices in companies, universities, administrations etc. The whistle-blower is usually an employee or customer and reports their own experience. They inform intermediaries and the media or the public directly. (Gabler's Wirtschaftslexikon)

WLAN (Wi-Fi) frequency band

Range of electromagnetic frequencies in which a wireless local area network operates according to the IEEE 802.11 standard. Such a network can be operated at different frequency bands (2.4 / 3.7 / 5 GHz), allowing a separation of traffic between two networks by using different frequency bands. (Own definition)

Bibliography

All links were checked on 15th February 2018.

1. Aktionsbündnis Patientensicherheit (Hrsg.): Handlungsempfehlung Anforderungen an klinische Risikomanagementsysteme im Krankenhaus, 2016, Im Internet: http://www.aps-ev.de/wp-content/uploads/2016/08/HE_Risikomanagement-1.pdf
2. Austrian Standards (Hrsg.): ONR 49000:2014. Risikomanagement für Organisationen und Systeme - Begriffe und Grundlagen - Umsetzung von ISO 31000 in die Praxis
3. Austrian Standards (Hrsg.): ONR 49002-3:2014. Risikomanagement für Organisationen und Systeme - Teil 3: Leitfaden für das Notfall-, Krisen- und Kontinuitätsmanagement - Umsetzung von ISO 31000 in die Praxis
4. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 100-1: Managementsysteme für Informationssicherheit
5. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
6. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
7. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 100-4: Notfallmanagement
8. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Glossar der Cyber-Sicherheit, Im Internet: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/cyberglossar_node.html
9. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT. Leitfaden, 2013
10. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT – Management-Kurzfassung, 2013,
11. Bundesärztekammer, Kassenärztliche Bundesvereinigung (Hrsg.): Bekanntmachung Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, Deutsches Ärzteblatt 2014;111(21):A963-72, Im Internet: https://www.aerzteblatt.de/pdf.asp?id=160315
12. Bundesärztekammer, Kassenärztliche Bundesvereinigung (Hrsg.): Bekanntmachung Technische Anlage, Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, Deutsches Ärzteblatt 2008;105(19):A1026-30, Im Internet: https://www.aerzteblatt.de/pdf.asp?id=60114
13. Bundesinstitut für Arzneimittel und Medizinprodukte: Empfehlung des BfArM, Risiken durch ungenügend abgesicherte WLAN-/Netzwerkschnittstellen bei Medizinprodukten, Referenz-Nr.: 3137/15, im Internet: https://www.bfarm.de/SharedDocs/Risikoinformationen/Medizinprodukte/DE/netzwerk_risiko.html
14. Bundespsychotherapeutenkammer (Hrsg.) BPtK-Leitfaden für Internetprogramme im Praxisalltag. Im Internet: http://www.bptk.de/uploads/media/BPtK-Leitfaden_f%C3%BCr_Internetprogramme_im_Praxisalltag_01.pdf

15. Deutscher Ärztetag 2017, Beschlussprotokoll, TOP II „Digitalisierung im Gesundheitswesen“, S. 246-300, Im Internet: http://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/120.DAET/Beschlussprotokoll_120_DAET.pdf
16. Deutsches Institut für Normung (Hrsg.): DIN ISO/IEC 27001:2017. IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen
17. Die Welt: System-Neustart am OP-Tisch, 11.04.2013, im Internet: https://www.welt.de/gesundheit/article160307851/System-Neustart-am-OP-Tisch.html?
18. eHealth Swiss (Hrsg.): Strategie eHealth Schweiz 2.0 (Entwurf vom 5.September 2017). OID: 2.16.756.5.30.1.127.1.1.5.1.1, Im Internet: https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/2017/D/170911_Entwurf_Strategie_eHealth_2.0_d.pdf
19. Europäische Kommission: Shaping the Digital Single Market, im Internet: https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market
20. KMA Online: Amazon will mit Expertenteam in digitale Gesundheitswirtschaft, Im Internet: https://www.kma-online.de/aktuelles/it-digital-health/detail/amazon-will-mit-expertenteam-in-digitale-gesundheitswirtschaft-a-35414
21. Krüger-Brandt H: Cybersicherheit als Herausforderung, Deutsches Ärzteblatt 2016;113(9):A364-9, Im Internet: https://www.aerzteblatt.de/pdf.asp?id=175147
22. Mertz M*, Jannes M*, Schlomann A*, Manderscheid E, Rietz C[t] , Woopen C[t] (2016) Digitale Selbstbestimmung. Cologne Center for Ethics, Rights, Economics, and Social Sciences of Health (ceres), Köln.
23. RP Online: Riesiger internationaler Cyber-Angriff trifft britische Kliniken, 12. Mai 2017, im Internet: http://www.rp-online.de/panorama/ausland/wanna-cry-riesiger-internationaler-cyberangriff-trifft-britische-kliniken-aid-1.6816373
24. Scherschel FA: Gehackte Medizintechnik: FDA will mehr Sicherheit durchsetzen, 19.01.2016, https://heise.de/-3075367
25. Schwan B: Mehr Sicherheit für Implantate mit Funkschnittstelle, 6.11.2013, im Internet: https://heise.de/-1972146
26. Springer Gabler Verlag (Hrsg.): Gabler Wirtschaftslexikon, Stichwort: Service Level Agreement, Im Internet: http://wirtschaftslexikon.gabler.de/Archiv/596505791/service-level-agreement-v5.html
27. Vollmar HC, Kramer U, Müller H, Griemmert M, Noelle G, Schrappe M.: Digitale Gesundheitsanwendungen – Rahmenbedingungen zur Nutzung in Versorgung, Strukturentwicklung und Wissenschaft. Positionspapier der AG Digital Health des Deutschen Netzwerks Versorgungsforschung e.V. (DNVF), Das Gesundheitswesen, 2017;79(12):1080-92
28. Windeck C: WannaCry: Gewaltiger Schaden, geringer Erlös, 14.05.2017, im Internet: https://heise.de/-3713689

Feedback

The APS Recommendations are intended as aids for improving patient safety. These aids need to be continuously developed and adapted to new innovations. Therefore, the APS expressly welcomes all types of feedback. If you notice inconsistencies, ambiguities or errors when you are using these recommendation, please do not hesitate to contact us. We are also very open to suggestions for improvement.

In addition, please feel free to contact the APS with questions that are not discussed in these recommendations.

Note: The editors regularly revise the recommendations every three years.

Please address your feedback, comments and questions to:

Aktionsbündnis Patientensicherheit e.V.
Am Zirkus 2
10117 Berlin
Germany
info@aps-ev.de

Imprint

Editors

Aktionsbündnis Patientensicherheit e.V. (German Coalition for Patient Safety)
Plattform Patientensicherheit Österreich (Austrian Network for Patient Safety)
Stiftung Patientensicherheit Schweiz (Swiss Patient Safety Foundation)

Working Group on Digitization and Risk Management

Chair
Strametz, Prof. Dr. Reinhard, Wiesbaden Business School, RheinMain University of Applied Sciences

Deputy
Jahn, Dirk, Dipl. Ing. biomed. Technik

Representative of the APS Board
Hardy Müller, Scientific Institute of TK for Benefit and Efficiency in Health Care.

Members of the Working Group and Authors of the Recommendations
Nico Brinkkötter (Krankenhausgesellschaft Nordrhein-Westfalen e. V.); Dr. Eike Eymers (AOK Bundesverband e.V.); Dr. Wolfgang Huf (Hietzing Hospital, Vienna Hospital Association) Altfried Inger (Verbund Katholischer Kliniken Düsseldorf); Dr. Alessa Jansen (Bundespsychotherapeutenkammer); Dr. Wolfgang Lauer (Federal Institute for Drugs and Medical Devices(BfArM)); Moritz Matschke (WELL IT); Frederik Meilwes (GRB Gesellschaft für Risiko-Beratung mbH); Oliver Steidle (Essen University Hospital); Dr. Stefan Wind (Apothekerkammer Berlin)

Acknowledgments
We gratefully acknowledge the support of the Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM, Federal Institute for Drugs and Medical Devices) and the Bundesamt für Sicherheit in der Informationstechnik (BSI, Federal Office for Information Security). We would like to thank Mr René Salamon.

Editorial Team
Prof. Dr. Reinhard Strametz (Wiesbaden Business School, RheinMain University of Applied Sciences), Dipl. Ing. Dirk Jahn, Hardy Müller, (Scientific Institute of TK for Benefit and Efficiency in Health Care), Dr. Wolfgang Huf (Hietzing Hospital, Vienna Hospital Association)

Second German edition: July 2018
First English edition: June 2019

DOI: 10.21960/201902/E

Layout: Alice Golbach (APS)
Photo credits: Fotolia.com/Paulista

Citation: German Coalition on Patient Safety (APS) e.V. (ed., 2018): Digitization and Patient Safety – R 1) Recommendations for Risk Management in Patient Care, Berlin

AKTIONSBÜNDNIS
PATIENTENSICHERHEIT

patientensicherheit schweiz

Plattform
Patientensicherheit