Chapter 17
Towards Guidelines for Medical Professionals to Ensure Cybersecurity in Digital Health Care

David Koeppe

Abstract There are no independent foundations and systems for general information security in medicine. For the special processing situations and in particular for the very high protection requirements of data and processes—ultimately health and life can depend on bits and bytes—a corresponding implementation of the essentially industry-independent procedure must take place. This topic is set to receive a special boost both among patients and among those responsible in the institutions because of the considerable increase in data protection awareness following the EU data protection basic regulation. This set of regulations addresses not only the lawfulness but also the security of the processing and threatens considerable sanctions in the event of gross negligence in this area. Regardless of whether this leads to the implementation of a proper information security management system in a larger institution—or whether the resources for such a large solution are not available in a small medical practice and it is instead sufficient for a successive long-term project to be processed—the topic must be addressed systematically.

Keywords Authorisation · Data protection · Information security management system · Patient safety

17.1 Introduction

17.1.1 Why Data Protection in Health Care?

What is the core motivation to seriously address security issues in data processing? In addition to the abstract insight into the advantages of taking precautionary measures, it is, above all, the fear of the disadvantageous incidents occurring that

D. Koeppe (✉)
Vivantes – Netzwerk für Gesundheit GmbH, Berlin, Germany
e-mail: david.koeppe@vivantes.de

M. Christen et al. (eds.), *The Ethics of Cybersecurity*, The International Library of Ethics, Law and Technology 21,
https://doi.org/10.1007/978-3-030-29053-5_17

may even result in the termination of one's own (business) activity. This focus on the business processes of classical information security has been expanded with an additional type of disadvantage, namely the legal sanctions imposed in the event of a failure of data protection because of the General Data Protection Regulation (GDPR) in the European Union that applies from 2018 onwards (see also Chap. 5). The adoption of suitable and appropriate cybersecurity measures now no longer depends solely on a personal sense of responsibility and on liability risks. Rather, it is actively demanded by the legislator.

From the perspective of data protection law, the physician or medical institution involved in data processing poses a risk for the person concerned (here: the patient) and his or her 'rights and freedoms'. In this respect, this perspective differs from that of traditional information security. In accordance with this significant increase in motivation prompted by the sanction regime of data protection law and based on the professional view of the author, the problem of cybersecurity in health care is here primarily approached from a data protection perspective. The contribution discusses the technical-organisational measures—also legally required (GDPR, Art. 32)—for the security of data processing.

17.1.2 The Problem

A (executive or freelance) physician, apart from his actual profession, hardly has a real chance of creating a state-of-the-art level of security in the processing of the patient data entrusted to him using his own specialist knowledge and his own resources. Either he works in a large organisation that guarantees cybersecurity for him, or he makes use of an appropriate service provider. However, this does not release him from his responsibility, especially since he has to make or confirm a number of specifications in a sophisticated information security management system.

The starting point of all considerations are the primarily medical and administrative requirements of opening one's own IT to 'the outside', in particular to other service providers, cost carriers and increasingly also to patients. This is a dynamic environment to which constant adjustments are necessary. In addition, the health ecosystem is currently undergoing rapid changes towards a patient-centred and technically increasingly ubiquitous landscape.

As a rule, information security cannot be designed from scratch, as health systems have their own history. The demand of dealing more intensively with cybersecurity usually arises during the day-to-day operations of an institution. It is based on amendments to the law (such as the GDPR), due to incidents or because of a general sensitisation towards the subject. Accordingly, at the beginning of all activities, an inventory of the existing processing methods and the system landscape is necessary. However, it does not make sense to stare at the cybersecurity dangers like a deer in the headlights. Without an overall view of processing security, only a patchwork would emerge. Thus, a checklist is not sufficient.

17.1.3 Setting the Framework

It should be emphasised at the beginning that, due to the proximity of the topics of cybersecurity and data protection, a joint processing of the respective requirements in a unified process and uniform documentation is urgently recommended. A separate consideration ultimately leads to considerable additional effort, since the same item is touched several times and potentially viewed and described in different ways. This involves the considerable risk of inconsistencies. Therefore, a combined approach to the data processing landscape, primarily from the broader perspective of data protection, is followed in this contribution.

A systematic and documented procedure is indispensable for assessing the completeness of the consideration as well as the appropriateness and effectiveness of the cybersecurity measures. Derived from the requirements of data protection law, there are essentially three elements:

– (Inventory and) Description of processing activities
– Risk analysis
– Design of measures

Essentially, these are the same elements required for a data protection impact assessment following the GDPR. This is a prescribed, formalised process to establish or ensure the legality and security of the processing of personal data. It is a generic process, whereas the peculiarities of the health care system usually require a very high level of protection for processes and data and that specific processing situations are considered.

17.2 Approach

From the perspective of classical information security, the focus is on processes, structures and technology. The view of data protection goes a little further and enriches the topic with legal and content-related aspects.

17.2.1 The Data Protection Perspective

From the perspective of data protection, the central subject to be described is ‘processing activity’. This is a process or a chain of individual processing steps that represents the logical totality of the handling of personal data that is required to achieve a purpose or bundle of purposes. Such processing activities include, for example, a clinical study, payroll accounting, diagnostics using a medical device, video monitoring in a sleep laboratory, or debt collection for defaulting debtors in health insurance. From a European point of view, the compulsory ‘Register of

Processing Activities' of the GDPR (Art. 30) provides guidance for structuring such activities. However, the minimum data specified there alone are not practicable; in addition, all available data that constitute the processing, e.g. with regard to the required transparency vis-à-vis the data subjects (Art. 12 ff. GDPR), should be collected centrally.

The mandatory information to be collected is as follows:

- Purpose(s) of processing (e.g. billing of services)
- Categories of data subjects and categories of personal data (e.g. patients and their master file data)
- Categories of recipients (e.g. internal: patient administration, external: insurance provider)
- Third country transfers and documentation of appropriate guarantees (e.g. Switzerland: adequacy decision of the EU Commission, India: use of EU standard contractual clauses)
- Deletion periods for the categories of data (e.g. billing data 10 years after the end of billing)
- General description of the technical and organisational measures taken to ensure the security of the processing (note: a reference to an existing security concept would be ideal here).

In addition, further information should be documented, in particular:

- Legal basis of the processing (e.g. for the implementation of the treatment contract pursuant to Art. 9 para. 2 lit. h GDPR)
- Origin of data (e.g. transmission from referring physician)
- If not obvious: description of the processing process with participants, interfaces, pseudonymisation levels, etc.
- Description of the measures to guarantee the principles of processing (according to Art. 5 GDPR)

The structuring of these activities for the purpose of description is the most demanding aspect to guarantee data protection and data security. It must be carried out in such a way that, on the one hand, all processing operations of the institution or the person responsible are actually recorded in their entirety and there are no 'blind spots' in the documentation. On the other hand, the handling of the individual processing activity should still be possible with a view to a meaningful description. The coarser while simultaneously more abstract the description, the lower the risk of overlooking something. At the same time, the associated complexity makes it difficult to create a comprehensible and functional description. Patient treatment as a single processing activity may make sense in a small medical practice, where all possible sub-processes (admission, diagnostics, findings, therapy, documentation, etc.) can still be potentially summarised in a single description. In a hospital, however, this would no longer be possible due to the complexity. Here, a modular decomposition into logical and self-contained sub-processes such as admission, medical diagnostics, medical and nursing documentation, discharge management, food supply, patient care service, archiving of treatment documentation etc. would be appropriate.

From a technical point of view, there is an obvious impulse to equate processing with the system (software, medical device) that is used for this purpose, to which manual activities are then added to complete the process description. This may be appropriate in individual cases, but in more complex processing environments, a specific software is often used for different purposes and thus for several processing operations and/or several applications, devices are required for one single processing. This requires adequate integration. For example, it makes sense to summarise similar processing operations in one description to avoid turning 100 blood glucose meters distributed over the hospital into 100 processing operations.

17.2.2 The Information Technology Perspective

A modularisation of the descriptions is urgently advisable in a more complex environment. Components or technical sub-processes that are repeatedly used, e.g. the institution's e-mail solution, the use of multifunction devices or simply the—ideally standardised—terminal (PC, smartphone) should be described and correlated with the relevant parameters in each case (technically and organisationally) to ensure they can then be referred to in the legal and functional context from the higher-level processing description.

With regard to information technology, the institution should be modelled. At least in larger institutions, this will have to be realised with appropriate software support, in order to be able to assign the components (software, terminals, servers, networks, rooms, personal groups) available in the underlying layers to each processing or business process (as a bundle of processing). Such a hierarchical model is indispensable for an information security management system. Appropriate handling will be possible, however, only with appropriate personnel and technical resources and thus remain rather reserved for larger institutions. A meaningful differentiation and grouping of components (e.g. networked PC versus stand-alone PC) can also be done manually in the medical practice.

To move from the rather abstract basics for security considerations to the practical conditions, the components that make up a processing activity must be analysed. From a purely technical point of view, these are the classic IT components such as servers, networks, end devices, operating systems, software, etc. However, the latest patch status helps little if the access door to the doctor's practice is not locked at the end of the day. Therefore, in addition to the technical layers in the narrower sense, other organisational aspects must also be considered.

17.3 Risk Analysis and Assessment

As soon as the systematic description has provided an overview of which elements of the IT landscape exist and what they are used for, the actual problems can be identified in a differentiated risk analysis.

Both the basic principles of information security (see also Chap. 2) as well as the data protection requirements for processing security (see also Chaps. 5 and 10) call for a risk-oriented approach. This enables scarce resources to be managed in such a way that only relevant risks are adequately addressed. However, a systematic risk assessment primarily contributes to ensuring that no hazards are overlooked (completeness of the risk model). A conscientious assessment of the identified risks based on this also provides the appropriate prioritisation for the following measures.

It is important to mention that risk assessment does not exclusively concern the risks for the operational information processing and thus the legal and economic interests of the physician. It also concerns the possible regulatory sanctions for breaches of duty. Thus, the European GDPR can now be regarded as decisive—regardless of the possible consequences for the patients (or employees) themselves. Essentially, three dimensions play a role here: warranty targets, protection requirements and threats.

17.3.1 Warranty Targets

The essential step before starting a risk inventory is the definition of warranty targets, i.e. the overarching aspects of data processing which should be protected against threats. The categorisations resulting from the different approaches are largely similar. There is not yet a European standard for the implementation of warranty targets from the GDPR. For the time being, reference is made here to the scheme of the 'standard data protection model' agreed upon within Germany by the data protection supervisory authorities (see https://www.datenschutzzentrum.de/sdm/ and Chap. 10 for details). The warranty targets provided for therein are:

- *Availability*
- *Integrity*
- *Confidentiality*
- Transparency
- Intervention capability
- Non-linkability
- Data minimisation

The objectives that are important for the security of processing in the narrower sense are availability, integrity and confidentiality (in italics), which are also the classic warranty objectives in information security. Thus, regardless of the different perspectives of operational information security and data protection, not only are the terms identical, but in the long run the measures to be taken are too. The four further objectives are primarily oriented towards the rights of the persons concerned and are initially ignored at this point, as they affect the risks for the persons concerned but less so cybersecurity, which is the focus here.

17.3.2 Protection Needs

The warranty targets relevant for cybersecurity are to be supported with measures depending on the risk. To achieve scalability here, a protection requirement is defined for each processing or for each data category to be processed, depending on the processing purpose and environmental conditions. It makes a considerable legal and practical difference whether an email (which per se contains personal references by sender and recipient) is used to order a catalogue of goods from a supplier or whether it is used to send a report of findings to another doctor. Usually, the level of protection required is normal, high and very high and can be defined as follows:

- 'Normal' stands for a personal reference that has hardly any potential for abuse or stigmatisation with regard to the individual concerned. Depending on the processing scenario, this can be simple contact data, a company telephone directory or the functional designation of a jobholder.
- 'High' would be a need for protection if the person concerned had an increased interest in the data not being disclosed, uncontrolled or misappropriated. This could concern the amount of salary, a bank account or a reference.
- A 'very high' need for protection must be provided for special categories of personal data and for data which are subject to a separate legal obligation to maintain secrecy—i.e., ultimately for all patient-related data arising in the context of health care or medical research.

This means that a very high need for protection for processing will usually have to be assumed in the health care system. Lower protection requirements will usually only arise in the handling of (most) employee data, information on relatives and in the B2B context (suppliers, service providers, colleagues from other institutions).

The category of data in connection with the category of data subject is not the only decisive factor for the classification. It also depends on the processing context. For example as soon as the absence of an employee is due to health reasons, the need for protection for confidentiality rises from normal to very high.

As is the case for the warranty targets, the protection requirements must also be presented from the perspective of those affected. The result is a matrix in which the need for protection is determined for the respective processing in relation to the warranty objectives. In simplified form, this could look as follows (Table 17.1):

Table 17.1 Example of a protection needs matrix

	Availability	Integrity	Confidentiality	…
Salary statement	High	High	High	
Data exchange with collaborating physician	High	Very high	Very high	
Patient record	High	Very high	Very high	

As far as possible, a qualitative or even quantitative assessment of the protection requirement categories is recommended in order to arrive at comprehensible definitions. For example, the integrity (e.g. in the case of manipulation/falsification of data) would have to be measured in the following cases: a) detection of the error is very likely, does not have major consequences and is easy to correct (= normal, e.g. wrong academic title in the salutation), b) detection of error has potentially temporary unpleasant consequences for the person concerned and a higher correction effort is needed (= high, e.g. incorrect payroll), c) danger to life or physical condition of the person concerned and errors possibly cannot be corrected (= very high, e.g. findings that serve as the basis for medication or surgery).

17.3.3 Hazards

To arrive at measures from the warranty targets (What must not be impaired?) and the need for protection (How in need of protection is it?), it is necessary to operationalise the hazards (What must I protect myself against?) as concretely as possible. These hazards must be related to the individual components (categories). A workplace PC faces other dangers than a cloud platform or a sonography device.

Many relevant hazards can be identified with systematic thinking in a rather simple process. However, it makes sense to use existing schematisations to avoid the risk of overlooking relevant aspects. The international standard for information security management systems is ISO 27001, which includes a catalogue of 'controls' for both processes and systems. However, the basic IT protection documentation (IT-Grundschutz-Kompendium; available at: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html; last access: July 72,019) of the German Federal Office for Information Security (BSI), which is similar in approach and freely available, is much more detailed and comprehensive. A complete implementation for the entire organisation would be a project of considerable scope. However, as long as there is no obligation to implement and no need for an audit, the relevant and/or interesting building blocks for one's own circumstances can be selected and successively worked through. The IT-Grundschutz-Kompendium currently contains 80 modules (e.g. 'Home Workstation', 'Web Browser', 'Clients under Windows 10', 'Remote Maintenance', 'Sensitization and Training'). For each module, there are hazard catalogues along with requirements (measures/guidelines/recommendations) graded according to protection requirement levels (basic, standard, increased). The 47 'elementary hazards' that are independent of the modules alone are a helpful catalogue for analysing an individual's situation.

As long as we move only between the three more technology-related warranty objectives of availability, integrity and confidentiality, there is usually no major difference in the result between the information security (facility-related) or data protection (affected-related) view. Ultimately, the data protection perspective in the basic protection system is an additional one which, by referring to the 'standard data

protection model' of the German data protection supervisory authorities, will in future offer an operational implementation of the requirements of the basic data protection regulation, above all with regard to the additional warranty objectives.

17.4 Design of Measures and Possible Conflicts

17.4.1 Balancing Measures

The risk analysis determines whether a measure should be taken in order to encounter a hazard that has been recognised and identified as relevant. The character and intensity of a measure depends on the requirement resulting from the risk in connection with the need for protection. It is not a question of maximising the protective effect but of appropriateness, which includes assessing the concrete circumstances of the processing, the state of the art and the implementation costs (see also Chap. 7). Excessive costs, however, do not speak in favour of foregoing processing security as such but rather in favour of foregoing this specific form of processing.

Data security measures do not only include obvious technical measures, such as installing a patch or activating an encryption feature. Organisational measures are also indispensable, especially when dealing with the human factor. Work instructions, restrictive allocation of authorisations, and the sensitisation and empowerment of employees are just as important and belong equally to an overall concept.

When designing measures, it is not only important to take the measure (e.g. data carrier encryption). Rather, a systemic perspective must be adopted to ensure that the measure is only taken if necessary. The mechanisms of an information security management system serve this purpose. In less complex environments, the proven PDCA cycle should be implemented at least: Plan-Do-Check-Act, i.e. a regular review with regard to the completeness of the risk inventory and assessment as well as the appropriateness and effectiveness of the measures with any necessary adjustments. In the case of significant changes in the processing or the environment at least, the continued legal conformity and thus the security of the processing should be checked.

It is advisable to consult a proven expert when designing measures in the technical environment. The correct configuration and administration of a firewall, a possibly mixed IT and medical technology network or a mail server should not take place at the amateur level—too much depends on it.

Finally, it is essential to document the measures to be taken and those actually taken based on the previous process steps. In addition, the justification for not taking a certain measure should be part of this documentation.

17.4.2 Data Security Vs. Patient Safety

IT disruptions can jeopardise the care of patients and, to a serious extent, their health. Carefully designed data security ensures that medical systems are protected against data loss and falsification or a considerable restriction of availability. However, it is possible that the measures to be implemented already affect the supply process and not the disruptions that are prevented by them. This creates a further level that must be included in the risk assessment. This view is most likely to be manageable if it follows the original design of the measures as a control loop.

An example of this would be a networked blood glucose meter that requires the entry of patient and employee IDs to ensure the traceability of the measurement and documentation process and to assign measured values to the correct patient. However, it must be technically possible at any time to carry out a measurement without an administrative lead-time, especially in medical emergencies. In such a case, an organisational determination would have to be made as to how the non-automatically assignable measurement values are to be addressed in the course of operations.

17.4.3 Authorisation Restrictions

In complex IT systems, a differentiated assignment of authorisations is necessary, not only from the point of view of confidentiality. Whereas in a small medical practice it is merely a matter of controlling certain functions in accordance with professional responsibilities and authorisations, in larger organisations particular attention must be paid to confidentiality. It is unacceptable that in a hospital, hundreds or even thousands of employees can access a patient record. Classical authorisation matrices have emerged, such as the authorisation of nursing staff for patients within their care units or the authorisation of physicians to the organisational units assigned to them, such as the specialist department and, at given times, also the emergency unit or specialist departments within the framework of night on-call services. In the course of increasingly variable treatment processes and increasing staff shortages, this simple basic principle of authorisation restriction is maintained increasingly infrequently.

The consequence of this is the urge to expand authorisations for being able to address any exceptional case in order to ensure the data are always available. Here, the argument of the ‘obstruction of work’ must not be given too much room at the expense of data protection; a relativisation of the articulated needs is often possible. Occasional requirements, e.g. on the part of administrative functions, can often be met by the division of labour processes, and in a great hurry, e.g. in the case of resuscitation, the physician also has better things to do than tackle an information system. A differentiated consideration is necessary, but in the end, a dampening of the safety effect by concessions to the work ability will have to be accepted.

A decisive element is how short-term adjustments of access can be made by the user administration, especially in the case of flexible personnel deployment. Automated approaches for the process-controlled and patient-centred assignment of authorisations exist in modern systems. However, this is still a dream of the future for most institutions whose static information systems are architecturally rooted in the 1990s.

17.5 Aspects Deserving Special Attention

Regardless of the requirement to carry out a systematic and area-wide examination of all aspects of cybersecurity, several 'classic' topics are often neglected in everyday data protection, although they can affect the security of processing. These aspects are often overlooked, especially in smaller institutions that lack the expertise and resources for a sound approach in the form of an information security or data protection management system. In the following, some of these aspects are outlined.

17.5.1 Data Transfer

As soon as the (electronic) release of data is concerned, a distinction has to be made between whether the data are transferred to a service provider who only processes them on behalf of the recipient (order processing in accordance with the GDPR, Art. 28) or whether it is a transfer in which the recipient pursues his own purposes with the processing. This could be a co- or aftercare provider, a cost unit, the holder of a research or quality assurance register, a patient transport service or a service provider of the patient who operates an electronic health record on behalf of the patient. In such cases, the transfer of the data also represents the transfer of responsibility (also under civil law). This means that—after ensuring the legality and a secure design of the transfer—the further responsibility lies with the recipient. As a rule, this also means that no further efforts are required to influence the recipient's processing circumstances, e.g. through data protection clauses in a cooperation agreement.

17.5.2 Order Processing of Data

If a service provider is commissioned with data processing that does not pursue its own content-related purposes, this falls into the domain of data protection order processing. An example could be a computer centre in which servers are hosted or applications are operated, a billing service provider, an envelope-inserting copy centre or a company that provides service and maintenance for IT, medical or office communication systems. Even if the data is not physically transmitted, order

processing must be carried out regularly in the case of (remote) maintenance if the service provider's activities could impair the achievement of even one of the warranty targets. The legal distinction between order processing and transmission can be difficult to make in individual cases, and the competent data protection officer should be consulted for advice.

The existence of order processing not only entails the obligation to conclude a highly formalised contract pursuant to Article 28 of the GDPR, but it also has a decisive significance for the allocation of responsibility. The client remains responsible for the processing and its legality, and for guaranteeing the rights of the data subjects. Accordingly, no contractor may be commissioned who does not offer the guarantee that he fulfils the requirements of data protection law—including those on data security—during processing. This must be checked before the order is placed and if necessary also during the course of the contractual relationship. As it is not possible to carry out more than superficial plausibility checks on the basis of one's own expertise, meaningful certificates or attestations by independent bodies should be demanded regarding the suitability of the service provider (in particular with regard to the security of the processing, e.g. in accordance with ISO 27001). A small typing office will not be able to offer this, but such certifications can be expected from a provider of cloud solutions. Certifications specifically relating to data protection exist sporadically, but the market will certainly develop a wider range of meaningful certificates in the coming years.

17.5.3 Mobile IT

A conventional, stationary IT environment is not easy to protect. However, as soon as mobile devices with possibly special mobile operating systems are added, additional and serious risks arise. Classic consumer devices are still hardly usable for operational use for processing health data. The presettings for synchronisation with the manufacturer's cloud, device location and the assumption that the device user would always be willing to transfer data to social media can hardly be mastered by an average user. Without the use of a restrictively set up mobile device management and an administration solution for restricting the possibilities while simultaneously processing risks of the end devices, the use of smartphones and tablets should be discouraged.

Another problem is the large and somewhat functionally tempting range of applications for communication and for medical use, and increasingly also for health professionals. In general, we can assume that the developers have maximised benefits and usability but were insufficiently effective in data protection and data security. In recent years, this has been confirmed by various studies on the security and data protection conformity of apps. Before using such applications (this also applies to web platforms and applications on stationary IT), the certification or at least the manufacturer's promise with regard to data protection and data security must always be checked. Otherwise, the following applies: Although the patients

may use such devices on their own responsibility, such an unexamined solution is unsuitable for professional use.

17.5.4 Internal Networks and Applications

The fact that IT components are operated in the premises of the institution does not mean that they are not exposed to any dangers and therefore do not have to be designed securely. Today, networking is omnipresent. Without a connection to the Internet, almost no information technology can be adequately operated. Whether for data exchange, for downloading patches and updates, or even for access by service providers, access to the Internet is nowadays technically and above all economically almost unavoidable.

However, it would be irresponsible to confine oneself to a single hurdle at the Internet access point (firewall, malware filter), since on the one hand hundred percent protection can never be guaranteed there and on the other hand dangers can also get into one's own network, e.g. by a data medium exchange. In recent years, there have been several examples where hospitals have had to do without core elements of their IT for days despite the usual protection mechanisms, due to malware.[1]

17.5.5 Communication with Patients

From the perspective of data security, the manifold possibilities for electronic communication with patients represent an increasing problem. It is not enough that patients increasingly expect health care professionals to use the e-mails, messengers and social media they have become fond of in other areas of life. Medical institutions also offer corresponding channels—partly in response to patient needs, partly on their own initiative. The fact that very few are suitable for communication with confidential information is often ignored or sometimes even not recognised.

Regardless of the patient's ignorance, indifference or simple comfort, the strict requirements for the integrity and confidentiality of data processing also and especially apply to communication via public networks by medical institutions. In any case, state-of-the-art transport encryption is indispensable, ideally end-to-end. This means that standard e-mail communication is already ruled out as a medium, unless an obligatory encryption technique is set up. However, most recipients cannot handle such an encryption technique. In addition, solutions of the platform operators and telecommunications service providers must meet the warranty targets obligatory

[1] See https://rp-online.de/nrw/staedte/neuss/neuss-computer-virus-legt-das-lukaskrankenhaus-lahm_aid-9614119 (last access 25.09.2018) or https://www.england.nhs.uk/2017/05/cyber-attack-updated-statement-and-background-information/ (last access: July 72,019).

for the health professional. The obligation to transmit all contact data in one's own database is, for example, a knockout criterion under data protection law for the use of a widely used, albeit end-to-end encrypting messenger.

It is advisable to offer patients a confidential digital communication channel in addition to telephone, fax and letter. Even if hardly anyone uses the PGP public key provided for email communication, it is still a signal to the interested public that inspires confidence.

17.5.6 Obligation to Report Data Breaches

If the efforts in data security have been insufficient and an incident occurs, there are regulatory consequences in addition to practical coping. Incidents in data or information security are frequently simultaneous violations of data protection. If personal data are disclosed unlawfully or unintentionally, destroyed, altered or lost, at least in the case of patient data, a reporting obligation to the data protection supervisory authority (Art. 33 of the GDPR) is necessary. In addition, the existence of an obligation to notify the persons concerned (Art. 34 of the GDPR) should also be assumed. Since failures to report or give notice in accordance with obligations are threatened with sanctions, the educational approach of the legislator to first understand these provisions as a deterrent should be appreciated by not underestimating efforts in data security from the outset.

17.5.7 Training, Awareness Raising and Instruction of Employees

The majority of data security problems are likely caused by human actions or omissions. Whether the cause is insufficient sensitivity, lack of knowledge or simply convenience—or a mix of these factors—this can and must be counteracted. Whether it is clicking on links in ominous e-mails, forgetting to make regular backups or simply misusing devices and software: from the perspective of the person responsible, these aspects also need to be considered—not just technical expertise in patient treatment. Serious errors or omissions can endanger the existence of both the facility and those affected by the data breakdown. Work instructions, user training and regular sensitisations are indispensable. This applies even if no information security management system necessarily draws attention to it.

17.6 Conclusion

Although ensuring data security is laborious and systematic processing within the framework of an information security management system, or at least on the basis of it, requires considerable work, it is nowadays an indispensable duty, especially in the health sector. The integrated processing of data protection obligations—underpinned by sensitive sanction threats—and the requirements of conventional information security are urgently recommended. Although this increases the complexity of the task, both have to be accomplished anyway. This results in considerable synergy effects through uniform documentation and the avoidance of time-delayed double consideration of the relevant aspects. Professional support from experts should be a matter of course, both in the conception of the procedure (to the extent appropriate to the size and complexity of the institution), in the processing, and not least in the design of the measures.

Nevertheless, the worst solution is doing nothing and hoping for the best. In any case, it is better to venture into the subject with work aids published by an expert and with the support of relevant advisers in the literature, and to fill the obviously largest gaps successively. In the course of dealing with the subject and growing sensitivity towards it, the willingness to ask experts for advice from a certain point will also increase. Ultimately, it comes down to a simple statement: patients would like to visit their doctor and be able to entrust him with their health and intimate secrets.