SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2024
ORGANIZATION AND MANAGEMENT SERIES NO. 192

INFORMATION SECURITY MANAGEMENT IN THE OPERATIONS OF HEALTHCARE ENTITIES

Paweł DOBSKI

Poznań University of Economics and Business; pawel.dobski@ue.poznan.pl, ORCID: 0000-0003-2267-9547

Purpose: The primary purpose of the study is to indicate the threats faced by medical entities in the context of the growing scale of collection and processing of personal data, including sensitive data. Therefore, it seems justified to attempt to systemically secure the processes related to this.
Specific objective: The main objective formulated in this way required further specification through the scientific and cognitive objective, which was to assess whether the implementation of the ISO 27001:2017 information security system in a medical entity allows for reducing the risk of information security incidents.
Project/methodology: The scope of scientific research defined in this way required the author not only to conduct literature studies, but also to apply appropriate research methods. As part of the considerations, it was decided to use methods such as: statistical analysis of data on the scale of implementation of a standardized data security system in the world and in Poland and the method of scientific description.
Results: The literature studies conducted and the research methods used allowed to demonstrate that the implementation of a standardized information security management system allows, by taking into account the requirements resulting from it, to increase the level of information security in medical entities. Identification of organizational, legal and ICT risks reduces the likelihood of information security incidents, and thus reduces the risk of exposing the healthcare entity to legal liability resulting from violation of the provisions of the Personal Data Protection Act (Journal of Laws of 2018, item 100) and the Regulation of the Parliament European Union and of the Council (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).
Limitations: A certain limitation faced by the author was the inability to take into account the number of ISO 27001:2017 certificates issued in medical entities both in the world and in Poland. This is due to the fact that certification bodies are not obliged to make such information public. Additionally, a certain limitation is the lack of reporting on compensation awarded by common courts to persons who have been harmed as a result of a breach of the protection of their personal data.
Practical implications: The study proposes a method for estimating risks in the field of information security in the activities of organizations, including healthcare entities. Additionally, the main benefits resulting from the implementation of the ISO 27001:2017 information security management system were indicated and the barriers that the manager of an entity providing health services should take into account were demonstrated.

Originality/value: There are a number of studies in both domestic and foreign literature on the information security system and its importance in organizations. Few authors make the effort to analyze this type of solutions in the context of providing medical services and the problems that must be solved by people managing medical entities.
Keywords: cybersecurity, information security incidents, information security system.
Category of study: scientific and cognitive study.

1. Introduction

Healthcare entities are faced with increasing requirements related to the collection, processing and use of personal data. This is primarily a consequence of technological progress and the increase in the scale of data collection. One should be aware that data regarding both staff and patients is collected not only in paper form, but also increasingly digitally. Therefore, securing access to them is becoming an increasing challenge. Whereas, when records were in paper form, it was enough to secure access to the rooms in which they were stored and the archives in which they were collected. With technological progress and the digitization process, there is a need to secure data stored on disks and servers. Additionally, it should be emphasized that more and more diagnostic equipment such as tomographs, mammograms and magnetic resonance imaging are digital devices that save patients' personal data, including test results, on disks. This requires securing access to them not only in the area of imaging or laboratory diagnostics, but also during their transmission not only to other organizational units within a given entity (e.g. hospital departments) but also to other medical facilities. It is therefore necessary to follow strict procedures for transferring this data only to authorized persons or organizations with which appropriate data entrustment agreements have been previously signed. It must be remembered that in the light of the Act on the Protection of Personal Data (Journal of Laws of 2018, item 100) of May 10, 2018, data regarding health and past diseases are defined as sensitive data, which means that they are particularly protected. Therefore, the role of the healthcare entity should be to take special care to protect these resources. This is problematic because the scope of collected data and the method of their processing are constantly evolving, so in order to have control over them, it seems necessary to implement an information security protection system in the healthcare entity.

2. Literature review

2.1. Cybersecurity incidents

While securing documentation in paper form does not require extensive knowledge and skills on the part of the organization's staff, selecting the optimal IT system, software or coding system for the company is no longer such a simple and obvious matter (Beskosty, 2017, p. 168). The increase in the scale of data collection and the development of information technologies increases the risk of cyber threats. The scale of threats may be confirmed by subsequent reports on the state of cyberspace security in the Republic of Poland. According to experts from the Government Computer Incident Response Team, the number of incidents related to cyber threats is growing and becoming more and more dangerous. A significant group are attacks carried out by the so-called botnets – computer networks infected with malware. The purpose of botnets is to carry out the orders of cybercriminals. The published reports of the Computer Security Incident Response Team operating at the Internal Security Agency show that while 6,236 attacks were recorded in 2018, most of which were attacks carried out by botnets, in 2019 there were 12,405 cyber incidents.

The consequence of this type of incidents is not only disruption of the functioning of the institution caused by blocking access to data, but also a threat to the health and life of citizens in the case of institutions that are part of the so-called critical infrastructure, which includes medical entities. Therefore, it should be assumed that ensuring information security should be included among strategic goals in every organization, especially one that has sensitive data (health condition, past illnesses, political preferences, sexual preferences, criminal record). Over recent years, and especially after the entry into force of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), awareness of the importance of information and the need to protect it have increased. The increase in the scale of cybercrime requires a methodical approach to ensuring information security. People managing organizations, including medical entities, should consider information as a resource as important as the others at their disposal, namely human, premises, financial and equipment resources (Beskosty 2017, pp. 163-164). Therefore, one of the solutions that can be adopted is the implementation of an information security management system (ISMS) in accordance with the ISO 27001:2017 standard.

2.2. Requirements and meaning of the ISO 27001:2017 standard

The ISO 27001 standard, like other standards, is subject to an amendment process. The currently applicable PN-EN ISO 27001:2017-06 standard replaced the earlier PN-EN ISO 27001:2014-12. These standards were developed based on previously developed protections in the industry. The report A Code of Practice for Information Security Management

published in 1992 by the UK Department of Trade and Industry can be considered the beginning of systemic information security. After 3 years, this document was included in the framework of the British standard BS 7799. After four years, in 1999, the first amendment to this standard was carried out, and a year later as part of the so-called "fast track", the international standard ISO/IEC 17799:2000 was published (Urbaniak, 2004, p. 367). This standard defined the requirements for securing organizations and IT systems in various security areas. In 2001, the British Standards Institution (BSI - the name of the United Kingdom's national standards body) issued the second sheet of the BS 7799 standard. This sheet defined the structure of an information security management system, which was consistent with, among others, the ISO 9001:2000 standard. This led to the publication of the ISO/IEC 27001:2005 standard.

In Poland, as well as around the world, a clear increase in interest in the ISO 27001 standard can be observed. This is due to the fact that managers are aware of the fact that the ISMS model, which is a set of good practices, allows for systemic protection of information. It should be noted that the number of ISO 27001 certificates issued worldwide has been gradually increasing since 2006, and a significant increase in dynamics can be observed since 2018. It can be assumed that this is a consequence of the entry into force on May 28, 2018 of the requirements arising from the Personal Data Protection Regulation (figure 1).

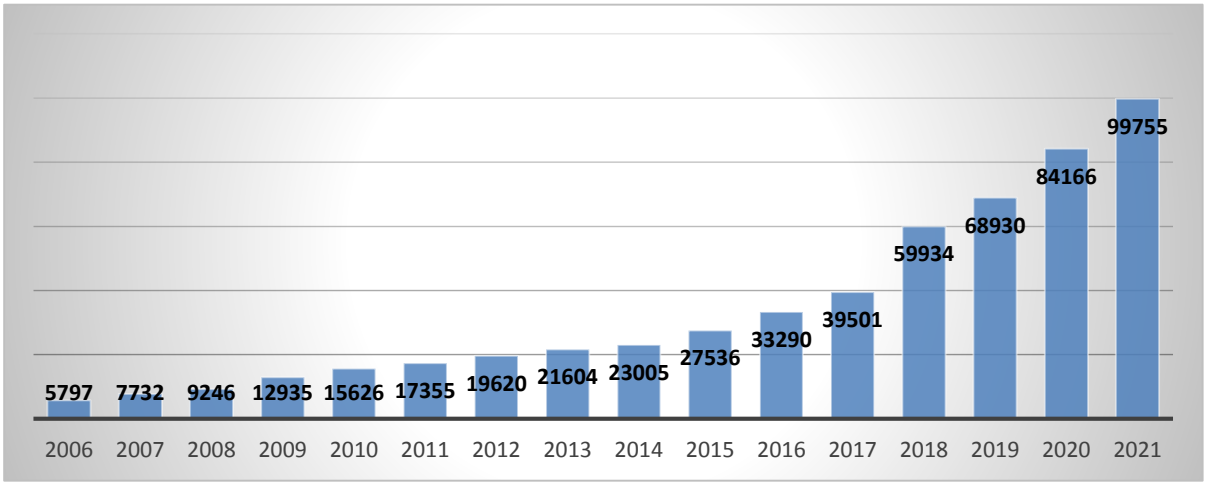

Figure 1. ISO 27001 certificates issued around the world.

Source: The ISO Survey of Management System Standard Certifications for 2007 to 2022.

For comparison, in Poland the dynamics of certificates issued seems to be higher than in the world. This applies especially to the situation in 2018, when this amount doubled compared to the situation in 2017 (figure 2).

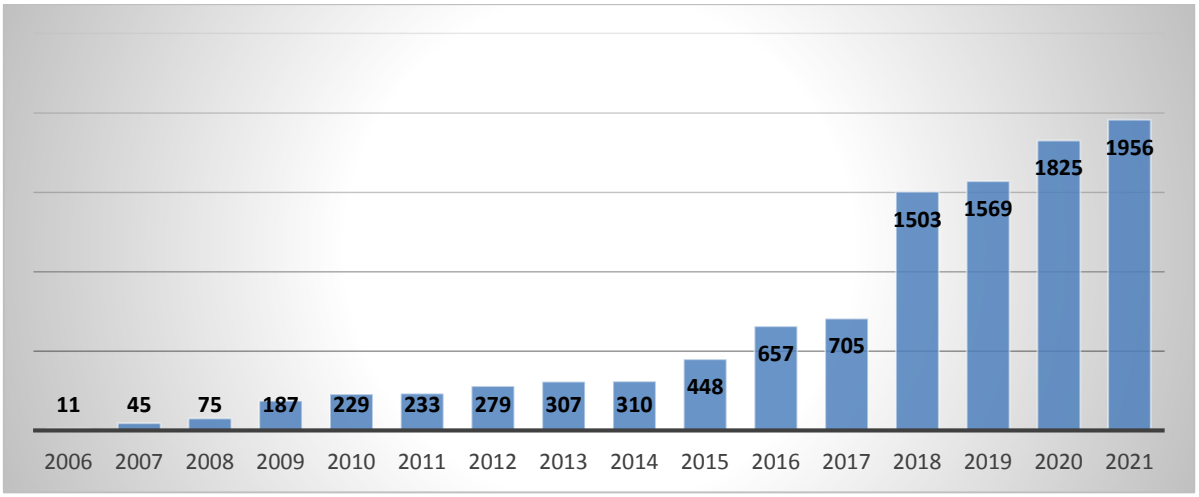

Figure 2. ISO 27001 certificates issued in Poland.

Source: The ISO Survey of Management System Standard Certifications for 2007-2022.

It is worth noting here that system certification is not obligatory and some organizations may implement the requirements arising from the standard without submitting to external assessment. A systemic approach to information protection seems more important. The ISO 27001:2017 standard indicates 3 aspects of information that must be protected:

- Confidentiality.
- Integrity.
- Availability.

Guaranteeing confidentiality means providing access to information only to authorized persons. Maintaining integrity is related to the accuracy and completeness of information, also during its processing. In practice, this means the need to verify the credibility of the information source and control over the changes introduced. Availability, in turn, requires ensuring that authorized persons can use the data when they need it.

Information security, as A Hamrol notes, may be at risk due to the lack or ambiguity of applicable procedures or human imperfection. The sources of threats may lie in management, hardware, software, as well as in the information itself. Threats may therefore come from (Hamrol, 2017, pp. 221-222):

- from a human, e.g. accidental deletion of a file, hacking into the system, including data theft (observations indicate that most problems regarding illegal access to information are related to the lack of knowledge of employees),
- from the environment (flooding, fire),
- from hardware (failure, incorrect configuration).

The aim of activities aimed at eliminating emerging threats, both in the enterprise and in the healthcare entity, is to achieve an organizational and technical level that will allow the development of continuous supervision mechanisms with the possibility of their process improvement (Olkiewicz, 2016, p. 91).

As M. Wiśniewska notes, organizations that want to effectively protect their information should use a systemic approach consisting in holistic management of their own information resources, the infrastructure used for their processing and the risks associated with information security. Thus, many organizations decide to implement a comprehensive Information Security Management System (Wiśniewska, 2009, p. 80).

Following the TQM philosophy in relation to information and IT areas may mean, in organizations such as healthcare entities, the creation of a TIQM (Total Information Quality Management) system, focused on the effectiveness, efficiency and security of information management. Comprehensive information quality management in organizations may be based on formalized and non-formalized systems of conduct resulting from, for example, international standards (e.g. ISO 27001). Adopting the TIQM approach means that managers must take into account (Olkiewicz, 2016, p. 93):

- customer orientation, including patient orientation,
- process orientation, including medical processes and accompanying standards,
- information orientation,
- preventive behaviors,
- continuous improvement.

Actions taken as part of the Information Security Management System should be focused not so much on reacting to information security incidents, but on prevention. Therefore, it is necessary to ensure an appropriate level of awareness in the healthcare facility, which seems to be particularly exposed to this type of threats due to the large number of staff working under time pressure and sometimes under severe stress. Additionally, especially in the case of public entities, financial limitations resulting from the level of contracting and the sometimes negligible involvement of the founding bodies have a significant impact on the possibility of implementing solutions. When implementing data protection solutions, you should also bear in mind that this applies to both paper and electronic documentation.

In healthcare entities, the issues with the greatest risk of information loss are solutions regarding access to premises, documentation and IT systems. Due to the above, the following security areas can be distinguished in medical service providers:

1. Legal and organizational security.
2. Physical security.
3. ICT security.

Ad. 1. With regard to issues related to the principles of handling information, it should be determined what information is most valuable to the medical unit and who is responsible for determining this value. It is also necessary to develop rules for information processing in the context of its marking, storage, destruction, copying and making it available externally. In the light of applicable regulations, it is very important to establish rules for reporting security incidents, which should be understood as an undesirable event constituting a breach of information security. Staff must be aware that incidents can occur in any organization,

and reporting and analyzing them is intended to protect the healthcare entity from similar or more serious situations in the future. Guaranteeing legal and organizational security also requires signing appropriate agreements with suppliers, including so-called entrustment agreements. This is important because the provisions of the GDPR assume the so-called joint and several liability and in the event of a leak of e.g. personal data through no fault of the healthcare entity, it may expose it to serious financial consequences. In a healthcare facility, it is also necessary to ensure that the staff only uses legal software and does not install any software on their own, including those that can be downloaded free of charge from the Internet.

Ad. 2. When raising issues related to physical security, the key issue seems to be ensuring the security of the area, facility and rooms. It seems justified to fence the area, install an electronic monitoring system, install anti-burglary foil in rooms, e.g. on the ground floor, and ensure facility protection. A separate issue is the appropriate organization of the reception desk or desk in the admission room. It seems necessary to ensure an appropriate distance between the person served and the person waiting in line. Additionally, remember that the content displayed on the monitor screen and entered into the documentation is not visible to unauthorized persons. The "clean desk" principle should be observed indoors (do not leave documents containing personal data when an authorized person has no control over them). The rooms must have locked cabinets (for documents), and access to them must require formal authorization (key policy). In the case of visitors, e.g. patients, a register must be kept or at least electronic supervision (monitoring). It is also justified to separate a visiting zone, which will guarantee that outsiders will not see who, apart from their loved ones, is currently hospitalized. Guaranteeing an appropriate level of physical security also requires monitoring access to the archive, for which a register of entries, exits and downloads must be kept. Documentation in the archive must be organized, e.g. in marked binders. Indoor temperatures and humidity should be monitored. Another aspect related to this area of security is also supervision over the operation of devices (computers, servers, etc.). First of all, access to them should be prevented by unauthorized persons (key policy). The premises must be protected against flooding or accidental damage (e.g. open window during a storm, equipment located near the air conditioner). In a medical facility, you should protect yourself against interruptions in the supply of electricity by using multiple lines, a power generator and a UPS. The server room should be air-conditioned to protect servers from overheating on hot days. The entire IT infrastructure must also be regularly maintained.

Ad. 3. When analyzing the issue of IT security, attention should be paid to maintaining a password policy. Changing passwords should be forced by the administrator, but there is no need to change them too often, because adopting such a rule may result in their weakening (password authors set one permanent password module and change some of them, e.g. by entering a number appropriate to the next month or year, e.g. stokrotka/01 in January and stokrotka/03 in March). The number of login attempts should be specified by the IT system administrator (logins cannot be shared) and anti-virus software should be guaranteed.

It is important to train staff in the safe use of Internet resources and to possibly disconnect computers that have particularly valuable information stored on their drives. As part of this type of threats, it is also necessary to introduce solutions that guarantee the creation of backup copies with appropriate frequency and to define the rules for the use of external media, the use of which should be limited or reduced to the use only of those that are registered (every fact of copying data is visible in the system). Additionally, it is necessary to meet certain rules regarding the destruction of data carriers and the method of their removal (the principle of, for example, overwriting data on computer disks).

Managing an entity within the TIQM concept concerns quality-promoting activities in the field of information and the overall functioning of the organization. It is impossible to separate the sphere of information security from the sphere of management. Aspects such as (Olkiewicz 2016, p. 94) become important:

- Constant monitoring of information quality (control, analysis and improvement of data obtained, processed and transmitted).
- Transparent, effective and understandable procedures that increase the role of information quality (strengthening the importance of employees, accreditation of accessibility security, etc.).
- Strengthening the information quality factor in the business sphere of the organization (monitoring and eliminating risk, creating appropriate IT and information security policies).
- Developing infrastructural and material resources (within IT) ensuring proper conduct aimed at shaping the quality of information.

It is worth emphasizing that the ISO 27001:2017 standard uses the previously described Deming model (PDCA), which should be applied to all ISMS elements. Approach process management assumes that all areas should be managed in such a way as to transform inputs into outputs.

The process approach to information security management provided in the standard pays attention to the identification, interaction and management of processes, i.e. (Norm PN-ISO/IEC 27001:2017):

- Understanding the information security requirements in the organization and defining information security principles and goals.
- Implementation and operation of security measures to manage information security risk in the context of the organization's overall business risk.
- Monitoring and reviewing the performance and effectiveness of the ISMS.
- Continuous improvement based on objective measurement.

The ISO 27001:2017 standard consists of two parts.

The main part contains requirements that increase the emphasis on the actual functioning of the organizations implementing the system. This is expressed, among other things, in the connection between planning and risk assessment (Chapter 6 of the standard) and the introduction of the organizational context, which forces managers of medical entities to conduct an analysis of the environment, taking into account strategic analysis methods, both in terms of the micro and macro environment.

Table 1.
Structure of the ISO 27001:2017 standard

Chapter	ISO 27001:2017
	Introduction
Chapter 1	Standard range
Chapter 2	Normative references
Chapter 3	Terms and definitions
Chapter 4	Organizational context
Chapter 5	Leadership
Chapter 6	Planning
Chapter 7	Support
Chapter 8	Operational activities
Chapter 9	Performance evaluation
Chapter 10	Perfecting

Source: study based on the PN-ISO/IEC 27001:2017 standard.

In terms of requirements, the ISO 27001 standard places particular emphasis on communication. It is necessary to take into account the type of information transmitted, the recipients of the message and the person responsible for its implementation. Estimating the risk of data leakage is also an important requirement. A sample spreadsheet is presented in Table 3, which identifies the risk within the implemented processes, then indicates its effects, determines the probability of occurrence and finally determines, as a result of the assessment, whether the risk level is acceptable or not. In the case of unacceptable risks, it is advisable to propose actions that will reduce the probability of occurrence or possible consequences.

Table 2.
Information security risk assessment sheet

Ordinal number	Process	Hazard description	The effect of the hazard (E) Scale 1-3	Likelihood of hazard occurrence (L) Scale 1-3	Risk of hazard occurrence R=ExL	Risk level	Comments
	Service in the emergency	Room Data leak	3	3	9	Unacceptable level	RODO training

Source: own study.

Additionally, in the case of risks identified as unacceptable, you can decide to introduce further actions (Table 3), which will allow you to specify the recommended corrective actions aimed at removing non-compliance or undesirable situations.

Table 3.
Plan for dealing with unacceptable risks

Ordinal number	Risk category	Description of the threat	Suggested corrective actions	Person supervising the implementation	Implementation date	Required costs	Implementation monitoring dates	Analysis of the effectiveness of actions

Source: own study.

A very important part of the ISO 27001:2017 standard is Annex A, which presents the areas of required security.

Table 4.
Security in the light of ISO 27001 requirements

	ISO 27001:2017
A5	Information security policies
A6	Organization of information security
A7	Human resources security
A8	Asset management
A9	Access control
A10	Cryptography
A11	Physical and environmental security
A12	Safe operation
A13	Communication security
A14	System acquisition, development and maintenance
A15	Relations with suppliers
A16	Information security incident management
A17	Information security aspects in business continuity management
A18	Compatibility

Source: Based on the PN-ISO/IEC 27001:2017 standard.

The process of implementing the Information Security Management System in accordance with PN-ISO/IEC 27001:2017 can be divided into the following stages (Dobska, Dobski, 2023):

Stage 1 - Preparation

When deciding to implement the requirements of the standard, you must first determine the scope of the system. In practice, this means deciding whether the implementation should concern the entire entity or only selected departments of the plant. The most advantageous approach, considering the scale of possible threats, seems to be to decide on implementation throughout the organization. The implementation process is complex and includes a number of stages that should be properly carried out in order to be considered effective (Wiśniewska, 2009, p. 82):

- preliminary audit,
- asset classification,
- developing a method and conducting a risk analysis,
- implementation of security measures,
- development and implementation of ISMS documentation,
- training for employees,
- internal audit and ISMS review.

The initial audit may be conducted by an employee of the healthcare facility or by a consultant from a consulting company. The involvement of an outsider seems justified because such a person, having experience from other organizations, will be able to notice problems that may not be noticed by an employee who has contact with given solutions in everyday work. The scope of the audit should cover all security areas included in the requirements of the ISO 27001:2017 standard. The result of such an audit is important in determining the scope of work that will need to be performed to prepare the entity for certification. During the audit, a wide range of information sources should be taken into account, such as documentation analysis, interviews with employees and observations. Observations and conversations seem to be particularly important because they will make it possible to verify the level of staff awareness of the importance of ISMS. It is worth observing whether employees do not enter data into the system using the login of co-workers, whether they follow the clean desk principle and whether they lock rooms when they leave them. Additionally, it is worth paying attention to the process of registering for tests or consultations. In addition, documents are an important source of information, including:

- reports from previously conducted audits (e.g. ISO 9001:2015 in the area of infrastructure supervision),
- organizational rules,
- management orders regarding document archiving and IT system,
- documentation in the field of IT,
- documents regarding the rules for handling information in the entity (e.g. office instructions),
- emergency instructions (e.g. actions in the event of fire, power outages, etc.).

During the audit, you can also verify the level of security of the area, buildings and IT systems.

Stage 2 - Development

A very important area of ISMS implementation is the classification of assets (devices, software, data, documents, etc.). First, you should conduct an inventory of assets and determine what the possible consequences of lack of access or possible loss of a given resource will be (e.g. what will be the consequences of a power outage, lack of Internet access, data leakage or failure). As a result of the inventory, you can start categorizing the following types:

1. Critical assets

Assets of this type should be considered those without which the medical entity cannot function, or the loss of which, as a result of providing access to unauthorized persons, would result in significant consequences. This category includes:

- servers,
- database,
- personal data sets (e.g. patients, employees),
- systems and software used in the process of patient service and reporting to the National Health Fund.

3. Valid assets

This type of assets includes devices and systems whose tasks can be performed by other means, but with additional effort and costs, or whose short-term unavailability does not result in serious consequences:

- network devices,
- backup and archiving devices and systems,
- devices supporting the operation of the server room (air conditioners, VPS),
- Alarm Systems,
- access control systems.

4. Core assets

The tasks of these assets can be performed manually with relatively little effort and resources. These types of assets include:

- desktop computers,
- laptops,
- telephones.

A very important aspect related to the classification of assets is to carry out a similar categorization of information. Due to the above, it is possible to isolate confidential information to which a narrow group of authorized persons has access. This type of information includes, for example, information about the health status of patients (test results, past illnesses, etc.). Another type of information would be internal information, which also has access to specific people, but it is a broader circle and is related to current activities. This type of information may include data regarding, for example, medical procedures performed as part of reporting to the National Health Fund. The last type of information is publicly available information. This type includes content available on websites (type and scope of services provided, staff employed in departments) and in information materials such as catalogs or brochures. In addition, it is also worth indicating data storage locations, including periodic and target data. In the case of patients' medical records, such as, for example, disease histories, they are initially stored in the ward where the patient is hospitalized, and after they are closed, they are transferred to the archive as their final destination. This, of course, involves defining appropriate rules for its security (including access restrictions) and transfer (including the time in which it should take place).

Carrying out activities related to the classification of assets allows for:

- improving the flow of information,
- protection against the risk of data being made available to unauthorized persons, including data theft,
- identification of possible causes of failure that may result in data loss.

Stage 3 - Testing

A very important stage of implementing the requirements of the ISO 27001:2017 standard is conducting a risk analysis. A reliable risk assessment requires time and commitment of the entire team. Risk estimation involves assessing the effects, the level of possible damage that may occur in the healthcare facility and its probability of occurrence. Therefore, in the context of risk categorization, it is necessary to determine the consequences related to the violation of data confidentiality, access to data and maintaining its integrity.

The next stage of implementation is to assess the level of security in the organization. This aspect very often exposes entities to costs related to the purchase of appropriate software (licenses) and the introduction of organizational solutions related to physical security (e.g. security, electronic monitoring).

When starting to create ISMS documentation, remember that its level of detail should depend on the nature of the business. Regardless of this level, its formalization must guarantee the definition of rules enabling information security.

The ISO 27001 standard specifies the following scope of documentation:

- documented information security policy,
- ISMS objectives,
- scope of ISMS,
- description of the risk assessment method,
- risk management plan,
- report with the risk assessment process,
- documented information supporting the ISMS,
- documented procedures needed to ensure effective planning, operation and control of information security processes and a description of the measurement of security effectiveness,
- required records (proof of implementation of activities),
- declaration of use.

Effective implementation of the requirements of the ISO 27001 standard is only possible with the participation of employed staff. Therefore, it is justified to conduct training dedicated to various professional groups. The first training, which should be attended by as many people as possible, is general training in the scope of the standard requirements. Thanks to this, employees can learn what the ISMS is, what are the conditions for its implementation and what is their role in the organization that implemented it. Additionally, the person conducting such training should present in an accessible way the benefits that will accrue not only to the entity, but also to individual people employed there. Subsequent training should be dedicated to representatives of individual organizational units. During this training, the structure of the documentation and the principles of its preparation should be discussed. The last of the training series is training for internal auditors, during which they learn the principles of auditing.

The person conducting such training in the form of a workshop should present the rules for developing working documents (e.g. a list of audit questions), preparing an audit plan and preparing an audit report. It may be helpful to explain what nonconformities are and how to classify them. Candidates for internal auditors prepared in this way can proceed to conduct internal audits on their own or with the participation of a consultant. Conducting audits and regular reviews of the ISMS (at scheduled intervals, point 9.3) allows not only to verify the effectiveness of the implemented solutions, but also the possibility of continuous improvement, which allows to increase the level of information security.

Internal audit, in terms of meeting the requirements of the ISO 27001:2017 standard, should be carried out in the following areas:

- documentation analysis,
- verification of the implemented level of information security,
- security of information processing in the context of the applicable Information Security Policy,
- ICT systems,
- personal data security training,
- conditions of ICT and network infrastructure,
- remote e-mail services,
- the advisability of implementing electronic document management.

The culmination of the activities carried out and proof of compliance of the introduced solutions with the requirements of the EN/SO/ICE/27001:2017 standard is the assessment of the certification body. A positive result of a certification audit can be not only a reason to be proud, but also an element that distinguishes a healthcare entity from others operating in a given area.

4. Effects

3.1. Benefits of implementing the ISO 27001:2017 standard for healthcare entities

The information security management system aims to ensure an appropriate level of resistance to disruptions and threats related to information security. As indicated by Malon Group (www.iso,org.pl downloaded on December 30, 2021), the basic benefits of implementing and using an information security management system consistent with the requirements of ISO 27001:2017 include (Dobski, Mikołajczyk, 2023, p. 131):

1. minimizing the risks related to data leakage resulting from the lack of data entrustment agreements (applies to cooperation, e.g. with companies servicing medical equipment recording digital data, such as computed tomography scans, magnetic resonance imaging, mammography machines),
2. the ability to effectively apply for public funds for the purchase of equipment (e.g. servers, UPS) and software (e.g. anti-virus systems),
3. preparing the organization for cybersecurity audits (applies to hospitals that have Hospital Emergency Departments),
4. elimination or reduction of the risk of events related to information security,
5. preparing the organization for events related to information security, including through appropriate procedures, effectively overcoming incidents when they occur - effective response, minimizing their impact on the organization,
6. pro-active approach to information security management by preventing the potential consequences of information security incidents, which may include:
   a) losses resulting from potential compensation for patients and stakeholders,
   b) penalties related to non-compliance with the provisions of law or regulations of civil-legal contracts,
   c) inability to carry out activities or individual processes and activities,
   d) loss of trust of patients and stakeholders - bad public relations, loss of the entity's reputation,
   e) effects resulting from sabotage activities carried out by employees,
   f) material and intangible losses resulting from disruptions in business continuity,
7. the implemented system increases the credibility of the organization in the eyes of patients,
8. improving the efficiency of processes and activities by regulating issues related to employees' access to appropriate and consistent information necessary from the point of view of the duties performed and assigned responsibilities,
9. ensuring an appropriate level of organization's resistance to business disruptions related to information security and effective event management in the event of a threat materializing,
10. meeting the requirements of the legislation in relation to the requirements of insurers,
11. ensuring the security of patient data as a result of a properly functioning information management system,
12. applying a risk-appropriate level of quality of protection for information assets,
13. order in terms of access to coherent and integral information and information circulation,

14. implementation and review of regulations regarding the security of personal data in terms of their adequacy to the organization's situation, the scope of processed personal data, integration with quality regulations,
15. meeting the requirements of the ISO 9001:2015 standard (in the case of entities that have already implemented the system) in terms of adapting the organization to new requirements.

When analyzing the benefits of implementing the system, it is worth mentioning the problems faced by plant managers:

- lack of employee understanding of the essence of the system, failure to follow recommendations and procedures, which results in incidents or undesirable events related to information security,
- downplaying the security area by managers and employees,
- lack of registration of incidents, which consequently leads to failure to implement corrective actions and data loss may result in customer complaints,
- lack of proper risk assessment regarding, for example, the information medium, the software used, the location - where the information is located, the information owner or user,
- lack of appropriate resources to implement the system - increasing costs may result in the temptation to not follow the system's recommendations.

Although security issues do not have to be related to applying for system certification, the standard is a document that enables systematic work on improving IT security.

3.2. Limitations of the implementation of the ISO 27001:2017 standard to healthcare entities

The implementation of the ISO 27001:2017 information security management system requires a number of expenses and staff involvement. For this reason, the person managing a healthcare facility must be aware of certain limitations and problems that must be faced:

- the need to incur expenditure on the purchase of equipment such as servers, disks on which backup copies will be saved, peripheral devices such as code readers, tablets,
- the need to create archives compliant with regulations in which documents will be stored and server rooms in which there will be servers on which digital data will be saved,
- purchase of professional virus software,
- staff training in the field of personal data protection,
- securing rooms and buildings against access by unauthorized persons,
- compliance with the rules resulting from the key policy,
- IT training to make employees aware of the scale of cyber threats.

5. Discussion

The content contained in the study is certainly not exhaustive and may serve as an inspiration for further considerations on cybersecurity and the importance of standardized management systems in increasing the level of data processing security. The protection of personal data of staff and patients is a big challenge faced by managers of medical entities. However, the fact of processing sensitive data imposes a number of obligations on the management staff related to compliance with the rules regarding both their collection and processing, including possible disclosure. The implemented Information Security System and the ISO 27001: 2017 certificate not only allow for a systematic approach to information security issues, but also raise the profile of the entity in relations with stakeholders. This is evidence confirming the high level of awareness in this area. However, the question arises whether in the situation of limited expenditure incurred on contracting services and a number of restrictions faced by the founding bodies of public medical entities (starostas and marshals) it will be possible to finance expenses related to the purchase of necessary equipment and staff training. It should be noted, however, that the implementation and certification of the ISO 27001:2017 Information Security System may be a consequence of cybersecurity audits carried out to which the so-called key entities, including those that have Hospital Emergency Departments (EDs) in their structures. In the author's opinion, the above-mentioned arguments seem to justify the efforts made by the staff of medical entities to implement the ISO 27001:2017 Information Security System.

Conflict of interest

No conflict of interest of the author.

References

1. Act of May 10, 2018 on the protection of personal data (consolidated text: Journal of Laws of 2018, item 100).
2. Beskosty M., (2017). Information security management. Security Studies. *Scientific papers of the Pomeranian University in Słupsk,* pp. 163-164.
3. Dobska, M., Dobski, P. (2023). *The role of standardized systems in the management of medical entities.* Difin, pp. 107-110.

4. Dobski, P., Mikołajczyk, J. (2023). *Trade management. Perspective of relations with stakeholders.* Poznań: Wydawnictwo UEP, pp. 114-131.
5. Hamrol, A. (2017). *Quality management and engineering.* Warsaw: PWN, pp. 221-222.
6. ISO/IEC 27000:2009 Information technology, security techniques, overview and terminology.
7. ISO/IEC 27002:2005 Information technology, security techniques, practical principles for information security management.
8. ISO/IEC 27003:2010 Information technology, security techniques, information security management system (ISMS) implementation guidance.
9. ISO/IEC 27004:2009 Information technology, security techniques, measurements.
10. ISO/IEC 27005:2008 Information technology, security techniques, information security risk management.
11. ISO/IEC 27006:2007 Information technology, security techniques, requirements for auditing and certifying authorities for information security management systems.
12. Olkiewicz, M. (2016). Management systems as a determinant of business information security. Security studies. *Scientific Journals of the Pomeranian University in Słupsk, no. 1,* pp. 91-94.
13. PN-EN ISO/ICE 27001:2017 Information technology - Security techniques - Information security management systems – Requirements.
14. PN-ISO/ICE 27001:2007 Information technology - Security techniques - Information security management systems – Requirements.
15. PN-ISO/ICE 27001:2014 Information technology - Security techniques - Information security management systems – Requirements.
16. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
17. Regulation of the Minister of Health of April 6, 2020 on the types, scope and templates of medical documentation and the method of its processing, Journal of Laws of 2020 of April 14, 2020, item 666.
18. Regulation of the Minister of Health of March 26, 2019 on detailed requirements to be met by the premises and equipment of an entity performing medical activities, Journal of Laws Laws of 2019, item 595.
19. Regulation of the Minister of Health of March 29, 2019 on the detailed scope of data covered by entry in the register of entities performing medical activities and the detailed procedure for making entries, changes in the register and deletions from this register, Journal of Laws of April 1, 2019, item 605.
20. Skolnik, K., Miciuła, I., Kubiński, P. (2018). *Information security management. Methodology, ideology, state.* Katowice: Science and Business, pp. 33-34.

21. Urbaniak, M. (2004). *Quality management. Theory and practice.* Warsaw: Difin, p. 367.
22. Wiśniewska, M. (2009). Comprehensive approach to information security management - information security management system. *Zeszyty Naukowe Politechniki Łódzkiej, No. 1064.* Łódź, pp. 80-82.