Wspolczesna Onkol 2011; 15 (5): 279–285

DOI: 10.5114/wo.2011.25656

Aim of the study: To analyse practical aspects of implementing the Personal Data Security Management System (PDSMS) in an oncology centre based on applicable legal requirements and professional standards.

Material and methods: The research method is based on the analysis of legal documents, quality standards, analysis of progress in the achievement of objectives of the PDSMS based on interviews with heads of units and on review of data protection documentation.

Results: The implementation of the PDSMS has caused the processed data to be adequately protected, minimised the risk of such data being used in a manner incompatible with their purpose, while ensuring the hospital's compliance with applicable legal regulations.

Conclusions: The implementation of the PDSMS has required technical and organisational measures to be taken in the centre's organisational units, in particular appointing data protection officers, engaging staff in the data protection process by awarding them with authorisations to process data and familiarising them with securities that have been put in place.

Key words: medical personal data, data protection, data security, security policy.

Practical guidance on implementation of the Personal Data Security Management System in an oncology centre

Mirosława Mocydlarz-Adamcewicz

Greater Poland Cancer Centre, Poznan

Introduction

In the era of the information society, data processing has become easier than ever. While providing many benefits, the removal of technical barriers supported with legal regulations has also brought some threats, as there is a growing interest in acquisition of private data. Such data are at risk of being accessed and used by unauthorised persons. The disclosure of personal details may, in turn, lead to the loss of patients' trust in a health care institution. Therefore, many health care institutions are putting more and more stress on protection of medical data processed by their IT systems. Data on health status, addictions or genetic code represent, under the Personal Protection Act, the category of personal data which are subject to special legal protection. Hence, each health care institution should put in place such an information protection system which will ensure confidentiality, integrity and accountability of processed personal data. This can be achieved through a properly implemented Personal Data Security Management System (PDSMS).

Aim of the study

The main aim of the study is to analyse practical aspects of developing, implementing and utilising a PDSMS in health care centres, based on applicable legal requirements and professional standards. The study presents chief security mechanisms (both technical and organisational) that should be put in place by a health care institution that processes personal data, particularly by means of IT systems.

Material and methods

The study provides a review of legislative measures, quality standards and available literature on protection of personal data in health care institutions. The situation in the Greater Poland Cancer Centre was also analysed with respect to PDSMS implementation in terms of technical and organisational security measures that have been taken by the centre, with particular stress on protection of personal medical data. Interviews were conducted with heads of units responsible for medical data protection in their respective departments with the focus on ensuring confidentiality of data processed in the hospital's IT systems. We analysed activities of IT System Administrators, whose responsibilities include guaranteeing the security of the centre's IT environment.

Results and discussion

Concept of personal data

Security is a concept with many meanings. In popular understanding, security is a state of being safe from threats. In the era of the information so-

ciety, security applies primarily to information in the context of IT systems. The PN-I-13335-1 standard defines IT security as all aspects related to defining, achieving and maintaining confidentiality[1], integrity[2], accessibility[3], accountability[4], authenticity[5] and reliability[6] of information, which is the most valuable asset held by each health care institution. Indeed, internal information processed by hospitals includes that of crucial importance for their activity, public policy or information representing personal data.

Personal data means all information concerning a specific person, by means of which – without much cost, time or effort – this person can be directly or indirectly identified, in particular by referring to an identification number or specific details determining his/her physical, physiological, mental, economic, cultural or social traits. With regard to the health services, personal data are not limited to identification details (name, surname and personal identification number), but also include medical information, such as that concerning patients' health condition (e.g. referrals, diagnosis results, delivered treatment procedures, nursing history, information sheet, follow-up), addictions or genetic code. Such data fall into a special category of personal details, known as sensitive data.

Data processing[7] is a commonplace activity at health care institutions. More and more often it is done using IT systems [1]. Therefore, implementation and operation of the PDSMS becomes necessary.

Appointment of data protection officers

The first step towards productive implementation of the PDSMS in the oncology centre was to appoint persons responsible for protection of personal data. The Personal Data Administrator (PDA)[8], responsible for ensuring technical and organisational protection of processed data (protecting data from being made available to unauthorised persons, illegally processed, changed or lost) delegated his duties to the Information Security Administrator (ISA) and IT System Security Administrator (ITSA). The ITSA supports the ISA in ensuring security of data processed in IT systems. Appointments were made by internal decision. Furthermore, roles and responsibilities within the organisational structure were established for the hospital director, managing staff (LISA[9], i.e. heads of departments, line managers, chief nurses), data processing officers (medical division, administrative division), security division (ISA, ITSA, ITA[10]), and physical security staff in the area of IT security.

With technology rapidly developing, it is the human factor that remains the weakest link of the security system. Therefore, appropriate selection of staff to be involved in personal data processing (physicians, nurses, psychologists, medical secretaries, administrative staff for human resources, pay roll, accountancy, financial settlement, statistics), IT administration (ITA), and data security (ISA, ITSA, LISA), became a strategic component of PDSMS implementation in our oncology centre. Information security largely depends on the staff's determination, knowledge and commitment in the process of PDSMS implementation. Proper organisation of security structures, distribution of roles, tasks and responsibilities between the hospital management and the personnel, particularly persons responsible for protection, forms the foundation of so-called trust systems [2]. The absence of the above-listed prerequisites might result in low reliability of the system, leading to IT security breaches.

Review and interpretation of legal acts

The next stage of designing the PDSMS involved development of an action plan for persons responsible for effective and efficient implementation of personal data protection. At its initial phase, the plan provided for the following measures:

1. Review and interpretation:

a) of national legal acts, including the Constitution of the Republic of Poland, relevant laws concerning personal data protection regulations and specific laws regulating the medical sector, providing specific implementing provisions for general rules contained in the Personal Data Protection Act [3]:
   - Act of 27 July 1997 on Personal Data Protection (*Ustawa o ochronie danych osobowych* – UODO),
   - Ministry of Internal Affairs and Administration Regulation of 29 April 2004 on Personal Data Processing Documentation and on Technical and Organisational Conditions to be Met by IT Devices and Systems Used for Processing of Personal Data (*Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych* – RDOiWT),
   - Act of 15 April 2011 on Medical Activities (*Ustawa o działalności leczniczej*),

[1]Confidentiality – a property of information ensuring that it is not made available or disclosed to unauthorised persons, entities or processes.
[2]Integrity – a property of information ensuring that it is not modified or destroyed in an unauthorised manner.
[3]Accessibility – a property of information that indicates its being available and possible to be used on request, in a pre-set timeframe and by an authorised entity.
[4]Accountability – a property ensuring that activities of an entity may only be explicitly assigned to that entity.
[5]Authenticity – a property ensuring that an actual identity of an entity is the same as declared.
[6]Reliability – a property indicating consistent and intended conduct and effects.
[7]Data processing means any operations performed on data. The concept of processing includes making available, changing, modifying, storing, transferring, collecting, recording and reworking.
[8]PDA – an authority, organisational unit, entity or person who decides on means and objectives of personal data processing. Should PDA be a health care centre, PDA's competencies are exercised by head of unit.
[9]LISA – Local Information Security Administrator is an independent manager and/or manager of the unit where data are processed. LISA is responsible for organisation of work and provision of adequate measures of personal data protection in his or her unit.
[10] ITA – IT Administrator, who plays a vital role in the Centre's structure with responsibilities including management of a separate part of the IT system, its effective functioning, protection of personal data processed in the IT system and network security.

- Act of 6 November 2008 on Patients' Rights and the Commissioner for Patients' Rights (*Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta*),
- Act of 5 December 1996 on the Professions of Doctor and Dentist (*Ustawa o zawodzie lekarza i lekarza dentysty*),
- Act of 5 July 1996 on the Professions of Nurse and Midwife (*Ustawa o zawodach pielęgniarki i położnej*),
- Ministry of Health Regulation of 21 December 2010 on Types and Scope of Medical Documentation and Methods of its Processing (*Rozporządzenie w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania*);

b) European Union and Council of Europe Acts, including in particular the Charter of Fundamental Rights, Convention No. 108, Directive 95/46/EC of the European Parliament;
c) ISO quality standards in the context of practical rules of information security management, in particular information security management in health care (PN-I 13335-1:1999; PN-ISO/IEC 27001:2007, PN-EN ISO 27799:2008);
d) professional codes, which – while not being legally binding – represent ethical models of conduct for specific professional groups: Medical Code of Ethics, Code of Professional Ethics of Nurses and Midwives, Code of Professional Ethics of Psychologists;
e) patients' rights with regard to protection of their privacy, access to contents of medical documentation and correction thereof, temporary or permanent termination of data processing: European Convention on Biomedicine, Lisbon Declaration on Patients' Rights, Charter of Patients' Rights.

2. Analysis of IT environment for personal data processing by taking stock of its elements:
a) mobile and stationary hardware (servers, arrays, computers, notebooks, monitors, printers);
b) passive and active network devices;
c) software;
d) carriers and back-up copies;
e) system documentation.

3. Risk analysis to identify those components of the IT system which require high level security measures and those which are not so critical [4] for the hospital, in particular:
a) identification of datasets (medical dataset, staff and pay dataset, health and safety dataset) and classification of data processed in them (non-sensitive, sensitive);
b) identification of sources and types of threats (internal, external), with an indication whether the threat is purposeful or incidental in nature (fire, flood, software breakdown, electricity breakdown, transfer of data to unauthorised parties, e.g. unauthorised patient's family, disclosure of temperature charts, interview with a patient in the presence of other patients);
c) establishing frequency of the threat and technical or organisational vulnerability, e.g. incorrect location of the IT system, lack of authentication procedures or back-up copy and data archiving management;
d) identification of effects (loss of confidentiality, integrity, accountability of data).

The development and implementation of a comprehensive PDSMS, i.e. a system covering all aspects of security, had to be preceded by analysis of legal and non-legal regulations in the area of information IT security. An in-depth analysis of both Polish legal regulations and EU directives contributed to the improvement in the quality of services provided by our institution [5] as regards security of personal medical data. It became a foundation of reliable risk and IT environment analyses. These, in turn, permitted identification of real threats for the system security in our institution, indicated areas requiring immediate protection, and ensured actions and protective measures to minimise the risk level acceptable for the hospital, thus preventing the IT security from being violated and addressing any possible adverse effects of such violations.

Protection of data processed in IT systems

The risk and IT environment analyses made in the hospital resulted in setting an IT security level. The security level in the oncology centre under study, according to the RDOiWT classification of security levels, was found to be high (Fig. 1).

Based on the above-mentioned analysis, a second stage of PDSMS implementation was put into action, involving definition and implementation of protective measures at the organisational, technical and physical levels. It comprised the following actions:

1. Designating a site for personal data processing, i.e. buildings, rooms, or parts of rooms where IT-based data processing is to be performed.
2. Developing and implementing personal data protection documentation as required by law and arising from good practice, including:
a) Personal Data Security Policy (PDSP),
b) Guidelines on Management of IT System to be used for processing personal data,

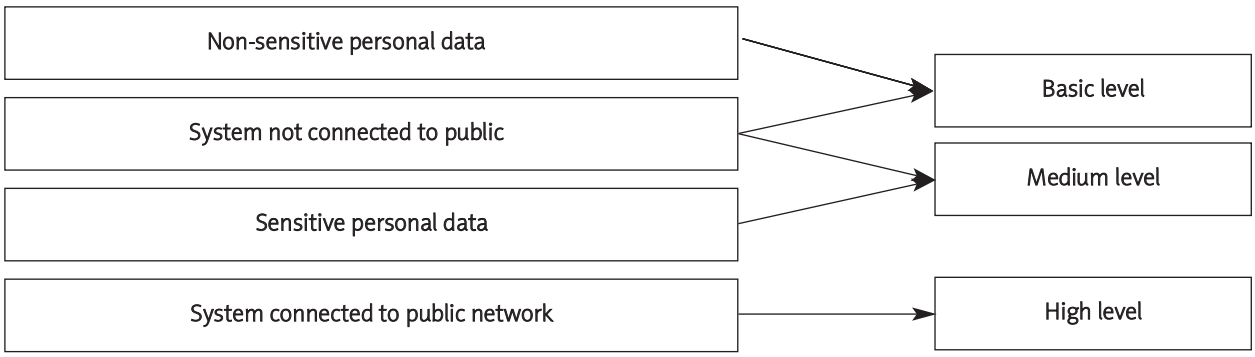


Fig. 1. RDOiWT Classification of security levels [6]

c) register of persons authorised to process personal data (Fig. 2),
d) authorisation to process personal data (Fig. 3),
e) non-disclosure agreements concerning received personal data,
f) rules of conduct in the event of an IT security breach[11],
g) request for award of IT system authorisations,
h) register of computers, user and administrator identifiers, administrative account passwords,
i) training programme.

3. Training for newly employed staff and regular refreshment training on applicable legal requirements, applied security measures, applicable personal data security documentation, liability for data processed.
4. Authorising hospital personnel to process personal data to the extent indicated by LISA (Fig. 2) and subject to their signing non-disclosure agreements concerning received personal data.
5. Publishing selected parts of the PDSP in such a way as to make it available for all staff involved in personal data processing (Internet, PDSP reports, guidelines for heads of units).
6. Developing guidelines for agreements to be made with servicing companies (processor) who are assigned to process data under software maintenance or hardware service contracts[12] (defining authorised persons, time and form of service to be provided: remote access or in-site service, liability and penalties for system security violations).

	ONCOLOGY CENTRE AUTHORISATION TO PROCESS PERSONAL DATA INFORMATION SECURITY ADMINISTRATOR (ISA) IT SECURITY ADMINISTRATOR (ITSA)	Version: 02.00. Date: 2008-09-01 Page: 1/1 Annex No. PDSP.F015 do PDSP

AUTHORISATION TO PROCESS PERSONAL DATA No. 12

NOTE:
This document is a property of the oncology centre. Changing, copying or disseminating without prior permission of the issuer is prohibited. Document for internal use only, made available to employees dealing with data processing, for tasks performed in this respect.

Pursuant the Article 37 of the Act of 29 August 1997 on Personal Data Protection (consolidated text Journal of Laws from 2002 No. 101, item 926) and under powers awarded to me by the oncology centre with regard to protection of personal data, I hereby authorise Ms/Mr*:

Kowalska, Anna
(surname, name)

to process personal data, including sensitive data* in the oncology centre, contained in:

Patient medical dataset
(name of dataset/domain)

necessary to perform duties related to the post/contract*:

Medical Doctor – Junior Assistant
(job title/contract)

in **Oncology Radiotherapy Department**
(name of unit)

in the period from **2009-02-08** to the **expiry of this authorisation**.

The above indicated person has been trained, is familiar with personal data protection regulations, and permitted to process data to the extent set out in the Act of 29 August 1997 on Personal Data Protection and its implementing provisions, and in the Head of the Oncology Centre internal regulation on personal data protection. The above indicated person is included in the Register of persons authorised to process personal data.

.....
(name and surname of authorised person)

.....
Information Security Administrator (ISA), IT Security Administrator (ITSA)

* – cross out as appropriate

Developed by	Checked by	Approved by
ITSA	ISA	PDA

Fig. 2. Register of persons authorised to process personal data

[11]Such rules are not directly required by the current legislation on personal data protection. They were developed at the Greater Poland Cancer Centre due to the requirement imposed on the IT Administrator to show particular diligence in protection of personal data.

	ONCOLOGY CENTRE REGISTER OF PERSONS AUTHORISED TO PROCESS PERSONAL DATA IN THE ONCOLOGY CENTRE IT SYSTEM SECURITY ADMINISTRATOR (ITSA)	Version: 02.00. Date: 2008-09-01 Page: 1/1 Annex No. PDSP.P015 do PDSP

REGISTER OF PERSONS AUTHORISED TO PROCESS PERSONAL DATA IN THE ONCOLOGY CENTRE

NOTE:
This document is a property of the oncology centre. Changing, copying or disseminating without prior permission of the issuer is prohibited. Document for internal use only, made available to employees dealing with data processing, for tasks performed in this respect.

Authorisation No.	Surname Name	Unit	Dataset	Date of training	Date of award (authorisations)	Date of expiry (authorisations)	Identifier	Date created (accounts)	Date removed (accounts)	ITSA signature	Notes
1.											
2.											
3.											

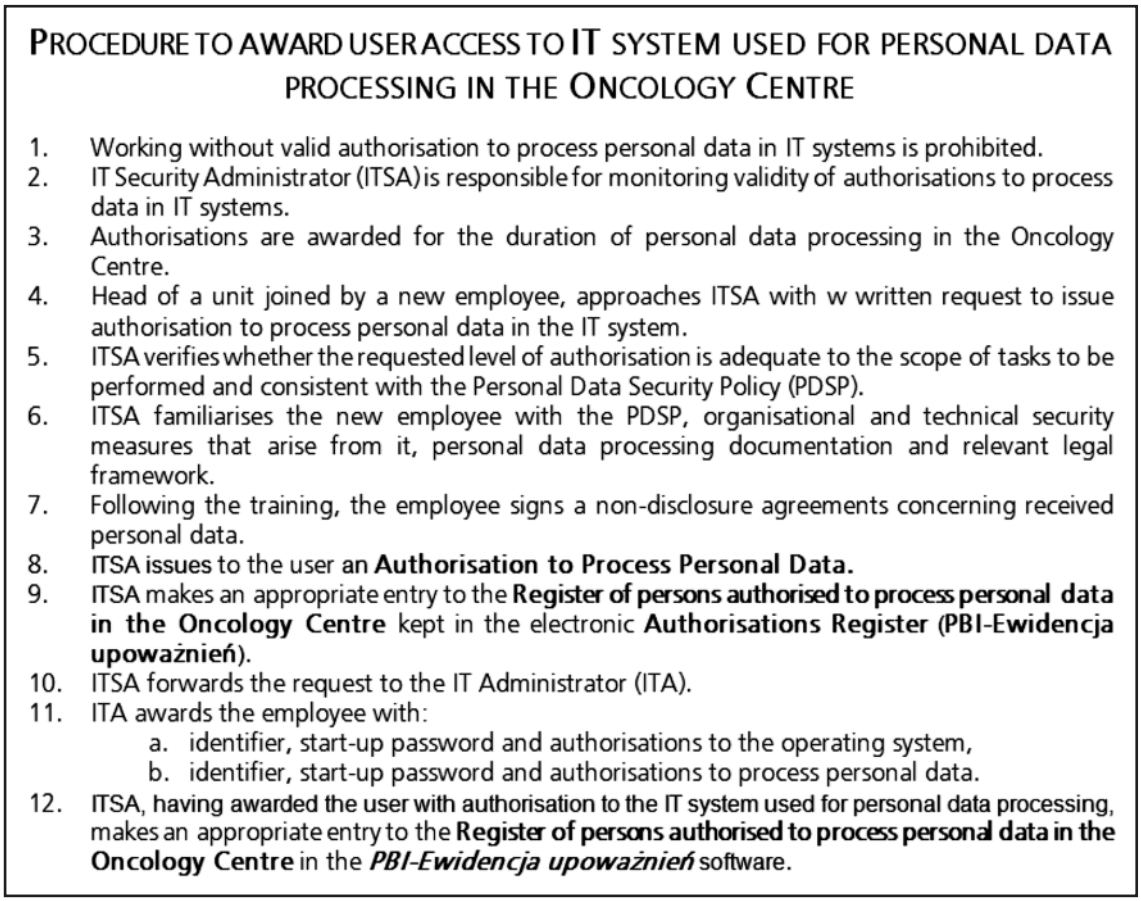
IT Security Administrator (ITSA)

Developed by	Checked by	Approved by
ITSA	ITA	ISA

Fig. 3. Authorisation to process personal data

7. Preparing and putting in place a list of physical protection measures to secure access to the sites of data processing, including rooms of strategic importance for the security system (server room, computer network hubs, Security and IT Department rooms): access control systems, burglar alarms, fire detectors, heat and humidity sensors, lockable doors and cabinets.
8. Separating the part of the IT system used for processing personal medical data from the rest of the hospital IT infrastructure and public telecommunication network.
9. Specifying rules of the personal data processing policy on the centre's stationary and mobile computers.
10. Selecting user identification and authentication mechanisms in IT systems (password, smart cards), developing procedures for managing such mechanisms, i.e. identifier and password policy, update frequency, complexity, procedures in case of authentication mechanism compromise, etc.
11. Developing procedures and putting into action measures to manage control of user access to personal data in the HIS[13] (minimum authorisation principle[14], necessary knowledge principle[15], task segregation principle[16] [7]) (e.g. the procedure to award user access to the IT system used for processing personal data in an oncology centre (Fig. 4).
12. Safeguarding working stations from harmful software, including by definition of antivirus and anti-spam policies.
13. Specifying rules of a software management policy with particular stress on software inventory, licence management, working station monitoring for legality issues, developing a list of standard software to be installed on working stations.
14. Defining security measures against theft, component replacement (passive security cables, locked cases, sealing).
15. Ensuring emergency power for computer hardware to prevent the loss of integrity [8].
16. Selecting and implementing encryption devices: encoding, decoding, digital signature [9].
17. Establishing rules for hardware repair and maintenance, in particular permissible response and repair time, repair documentation: hardware delivery and receipt reports, service notification register.
18. Establishing procedures for management of personal data carriers and creation and storage of back-up copies (schedule indicating type of copy, carrier labelling, back-up procedure, time and place of storage).
19. Implementing the clear screen principle which consists in setting monitors in such a way as to prevent infor-

[12]A contract for assignment of personal data processing has to be made in writing with a specified objective, scope, object, persons authorised to process data, responsibilities of parties, security measures used, verification and identity check of service persons.
[13]HIS – Hospital Information System.
[14]The minimum authorisation principle involves the award of minimum authorisations necessary to perform tasks assigned to a specific post.
[15]The necessary knowledge principle involves the award of only such authorisations as are necessary to perform specific tasks.
[16]The task segregation principle involves the award of limited authorisations which do not allow performance of the whole task by one person only.



PROCEDURE TO AWARD USER ACCESS TO IT SYSTEM USED FOR PERSONAL DATA PROCESSING IN THE ONCOLOGY CENTRE

1. Working without valid authorisation to process personal data in IT systems is prohibited.
2. IT Security Administrator (ITSA) is responsible for monitoring validity of authorisations to process data in IT systems.
3. Authorisations are awarded for the duration of personal data processing in the Oncology Centre.
4. Head of a unit joined by a new employee, approaches ITSA with w written request to issue authorisation to process personal data in the IT system.
5. ITSA verifies whether the requested level of authorisation is adequate to the scope of tasks to be performed and consistent with the Personal Data Security Policy (PDSP).
6. ITSA familiarises the new employee with the PDSP, organisational and technical security measures that arise from it, personal data processing documentation and relevant legal framework.
7. Following the training, the employee signs a non-disclosure agreements concerning received personal data.
8. ITSA issues to the user an **Authorisation to Process Personal Data.**
9. ITSA makes an appropriate entry to the **Register of persons authorised to process personal data in the Oncology Centre** kept in the electronic **Authorisations Register (PBI-Ewidencja upoważnień).**
10. ITSA forwards the request to the IT Administrator (ITA).
11. ITA awards the employee with:
    a. identifier, start-up password and authorisations to the operating system,
    b. identifier, start-up password and authorisations to process personal data.
12. ITSA, having awarded the user with authorisation to the IT system used for personal data processing, makes an appropriate entry to the **Register of persons authorised to process personal data in the Oncology Centre** in the ***PBI-Ewidencja upoważnień*** software.

Fig. 4. Procedure to award access to IT system used for personal data processing

mation displayed in them from being seen by other persons, using password-protected automatic screen savers and locking working stations or applications on user's request.

20. Following the clear desk principle whereby documents containing personal data cannot be left unattended at places accessible to unauthorised persons.
21. Complying with the requirements of sec. 7 of RDOiWT, in particular concerning the registration of: date of first entry of data into the system, user identifier, source of data, date of reported concern, possibility for processed data to be printed out in a commonly understandable form.
22. Meeting requirements concerning information and right to control of one's personal data, pursuant to Article 24, 32-35 UODO.
23. Implementing principles of awarding access to personal data to third parties in the light of UODO and its detailed implementing regulations for health care.
24. Responding to incidents, investigating their causes and addressing their effects.
25. Periodic security and IT environment controls and audits with regard to effectiveness and efficiency of security mechanisms and PDSP compliance.

Implementing the PDSMS in health care institutions is a duty and necessity arising from both the Personal Data Protection Act and relevant health care regulations. The right to privacy and the right to decide on one's personal data are guaranteed by the Constitution. In view of the above, each Personal Data Administrator should take such measures as may be necessary to prevent intended and wilful actions, but also incidental events [10], posing a threat to IT data processing IT. It is then necessary to define and implement measures ensuring security of datasets. The choice of the above-mentioned measures by the Greater Poland Cancer Centre meets the technical and organisational requirements laid down in UODO with regard to preventing data from being accessed by unauthorised parties, illegally processed, changed, lost or destroyed, as well as defining physical security measures. Furthermore, the Centre's user control system [11] and personnel training enable implementation of a resilient PDSMS that has to be periodically reviewed, following the security consultant Bruce Schneider's words that "security is not a product, but a process" [12].

Conclusions

Effective implementation of the Personal Data Security Management System in health care institutions depends on the efficacy of a legal and organisational framework. There is, beyond any doubt, a strong tendency to develop security systems for medical data. This, however, requires an action plan for a hospital with due emphasis put on:

1) analysis of legal and non-legal acts regarding protection of personal data and professional regulations applicable to health care institutions,
2) promotion of achievements in terms of information security to allow a change in the awareness of data protection needs among hospital personnel and managing staff,
3) appointment of persons responsible for personal data protection with specified roles and action plans,
4) identification of threats, selection and implementation of organisational and technical protection measures appropriate to the accepted security level,
5) improvement of employees' knowledge and skills through a training system and personal data security documentation.

References

1. Kaczmarek A. Obowiązki administratorów danych osobowych przetwarzających dane osobowe w systemach informatycznych rejestrujących usługi medyczne. Konferencja naukowa, Warszawa 2000.
2. Standardy NIST: http://www.nist.gov, standardy CCITT, standardy PN.
3. Serzycki M. „Gazeta Wyborcza" pyta o zabezpieczanie danych w służbie zdrowia (12.11.2009).
4. Gałach A. Instrukcja ochrony danych osobowych w systemie informatycznym. Gdańsk 2004.
5. Bogusz-Czerniewicz M. External review systems for radiation oncology facilities – clinical audit versus other review systems. Rep Pract Oncol Radiother 2009; 14: 11-7.
6. Pilc B. Ustawa o ochronie danych osobowych. Materiały wykładowe UKSW PSOIN, Warszawa 2008.
7. Galach A. Ochrona danych osobowych w systemach teleinformatycznych. Materiały szkoleniowe, JDS Consulting, Warszawa 2008.
8. Drozd A. Zabezpieczenie danych osobowych. Presscom, Wrocław 2008.
9. Janowski J. Podpis elektroniczny w obrocie prawnym. Warszawa 2007.
10. Polok M. Bezpieczeństwo danych osobowych. Warszawa 2008.
11. Nałęcz M. Biocybernetyka i inżyniera biomedyczna 2000. Systemy komputerowe i teleinformatyczne w służbie zdrowia. Akademicka Oficyna Wydawnicza Exit, Warszawa 2002.
12. Mitnick K. Sztuka podstępu. Łamałem ludzi, nie hasła. Helion, Warszawa 2003.

Address for correspondence

Mirosława Mocydlarz-Adamcewicz
Greater Poland Cancer Centre
Garbary 15
61-866 Poznań
e-mail: miroslawa.mocydlarz-adamcewicz@wco.pl