PERSONAL DATA PROTECTION

MATERIAL FOR STUDENTS AND APPRENTICES

UNIWERSYTECKI
SZPITAL KLINICZNY
im. Jana Mikulicza-Radeckiego
WE WROCŁAWIU

Introduction

University Clinical Hospital in Wroclaw, hereinafter referred to as the Hospital, is one of the leading treatment and research centers in the country with an established position, providing diagnostic, treatment and consultation services within the public healthcare facility system. It cooperates with many partners in Poland and abroad. To perform its tasks, the hospital uses modern IT systems, which makes it fully dependent on the smooth operation of these systems.

The essence of all activities of the University Clinical Hospital in Wroclaw is to protect the life and health of patients.

Respecting the fundamental right of every human being to privacy, the Hospital attaches great importance to ensuring the confidentiality and protection of the processed personal data, and makes every effort to ensure that the processing of such data is carried out in accordance with the law, as well as with respect for the fundamental rights and freedoms of data subjects.
In order to meet the above, the Hospital trains people who process personal data so that they have the necessary knowledge in the field of personal data protection.

The Hospital is an unit authorized to educate students of medical sciences, doctors and other medical personnel, therefore these persons may be present when providing health services and are entitled to access medical records, only to the extent necessary to achieve the educational goals.

The Student / Apprentice is obliged to keep confidential the personal data obtained in connection with participation in the classes at the Hospital (regardless of the method of obtaining them - written, electronic, oral), both during the classes and after they are finished.
Students / Apprentices preparing to practice a medical profession are required to read this training material.

This training material was prepared in connection with the implementation of the tasks of the Data Protection Officer resulting from the provisions of art. 39 sec. 1 point b) GDPR - awareness-raising activities, training of persons participating in personal data processing operations.

The training material for Students / Apprentices does not constitute an interpretation of the law on the protection of personal data and is of an informative and training nature only.

Andrzej Michalski - Data Protection Officer

Content
Introduction

1. What does GDPR stand for

GDPR (General Data Protection Regulation) means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/45 / EC (general regulation on the protection of personal data).

One of the goals of the general regulation on the protection of personal data is to harmonize the provisions governing the protection of personal data in EU countries, as well as to standardize the way data flows between these countries.

The GDPR protects the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data.

The GDPR comprehensively regulates the issues of personal data protection and has been applied since May 25, 2018 in all EU Member States.

The full text of the GDPR is available at: https://uodo.gov.pl/en/514/1055

The polish legal act that supplements the regulations on the protection of personal data is the Act of May 10, 2018 on the protection of personal data. The Act does not duplicate the provisions of the GDPR, but only complements the GDPR, to the extent that the EU legislator has allowed for the clarification of certain issues under national law.

The text of the Personal Data Protection Act is available at:
https://uodo.gov.pl/en/479

2. Personal data – what does it mean

Personal data is any information relating to an identified or identifiable natural person ("data subject").
An identifiable natural person is a person who can be directly or indirectly identified, in particular on the basis of an identifier such as name, identification number, location data, internet identifier (IP address, e-mail address) or one or more specific factors defining the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person.
This is all the data that allows you to identify a person in the physical and virtual world.

Data subject - a natural person who can be identified on the basis of specific personal data.

An identified person is a person whose identity we know, who we can indicate from other people.

Unidentified person is one whose identity we do not know, but we can know by using the means (data) we have.

Examples:

- identified person: patient whose data is processed by the hospital; an employee whose personal data is processed by the employer; a student whose data is processed by the university.

- identifiable person: doctor / nurse with license number we know the profession; a student whose album number and the name of the university are known.

There are the following types / categories of personal data:

a) special categories of personal data (also known as sensitive / sensitive data) The special categories of personal data include:

- data revealing racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- genetic data,
- biometric data,
- health data,
- sexuality or sexual orientation

b) **the so-called ordinary personal data,** e.g.

- Name and surname,
- PESEL,
- home address,
- date
- of birth, gender,
- parents' names,
- education,
- e-mail address, telephone number,
- ID number and series,
- internet login.

3. How does the GDPR define health data

Health data is all data about the health of the data subject. Data related to health means personal data related to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status.

Personal data concerning health should include **all data concerning the health status of** a natural person, which reveal information **about the past, present or future** physical or mental health of the data subject.

Such data include:

- information about a given natural person collected **during his registration for healthcare services or during the provision of healthcare services to him,**

- a number, symbol or designation assigned to a given natural person for the purpose of unambiguous identifying that person for health purposes;

- information **from laboratory or medical tests** of body parts or fluids, including genetic data and biological samples; • all information, e.g. about the **disease, disability, risk of**

- **any information about illness, medical history, clinical treatment or the physiological or biomedical condition of** the data subject, irrespective of its source, which may be, for example, a doctor or other healthcare professional hospital, medical device or in vitro diagnostic test.

Data on the health of the Hospital's patients, including data contained in medical records, belong to special categories of personal data and are subject to special legal protection.

4. What does the processing of personal data mean

Processing means an operation or set of operations performed on personal data or sets of personal data in an automated or non-automated manner, such as:

- collecting,
- recording,
- tidying up,
- storage,
- adapting or modifying,
- downloading,
- browsing,
- exploitation,
- disclosure by sending,
- disseminating or making available in any other way,

- matching or linking,
- limiting,
- removal or destruction.

The catalog of activities that may constitute the processing of personal data is an example, it is an open catalog - it should be assumed that the processing of personal data is any activity that we perform using personal data (all operations performed on personal data) in order to achieve a specific goal processing.

Familiarization (viewing, reading) by Students / Apprentices of the data contained in the patient's medical records for didactic purposes also includes the processing of personal data.

5. How does the Hospital process personal data

The hospital processes personal data:

- traditionally (paper documentation) - it includes, among others: medical documentation, test results, personal files of employees, printed documents containing personal data.

Examples of the activities processing: filling in medical documentation, of storing, viewing, copying, organizing, sharing, destroying.

- electronically - in IT systems, eg patient data in the HIS system (electronic medical documentation), patient data stored in the memory of medical devices / apparatus.

Examples of processing activities: entering data into the system, saving, searching, copying, modifying, downloading, saving, organizing, deleting.

Personal data is protected regardless of how it is processed.

It does not matter how they are used or stored - whether we use the latest IT system or paper documents in binders / folders, files, books, lists, records - in each of these cases, data processing is subject to the requirements of the GDPR.

6. Who is the Administrator of the data processed by the Hospital

The term "Administrator" means the natural or legal person, public authority, agency or other body that alone or jointly with others determines the purposes and means of the processing of personal data.

The administrator of data processed at the Hospital is:

University Clinical Hospital in Wroclaw
ul. Borowska 213
50-556 Wroclaw

The data administrator is represented by **the Director of the Hospital,**

The Administrator determines the purposes and methods of personal data processing, and is also obliged - taking into account the nature, scope, context and purposes of processing as well as the risk of violating the rights and freedoms of natural persons of varying probability and severity of risk - to implement appropriate technical and organizational measures to process personal data took place in accordance with the GDPR.

7. Who is the Data Protection Officer

The Data Protection Officer (DPO) is a person appointed by the Director of the Hospital who supervises the observance of the principles of personal data protection in the Hospital. The DPO is appointed on the basis of professional qualifications, in particular expertise in data protection law and practices, and the ability to fulfill the tasks referred to in Art. 39 GDPR.

At the Hospital, **Mr Andrzej Michalski** was appointed Data Protection Officer

Contact details of the DPO:

email address: iod@usk.wroc.pl

direct telephone number (71) 733 1791

In the organizational structure, the Data Protection Officer reports directly to the Hospital Director.

8. Who is the IT System Administrator

The IT System Administrator is an employee of the IT Department of the Hospital, with appropriate administrative rights to the system, responsible, inter alia, behind:

- technical and organizational service of the IT system,
- IT system administration,
- database administration within the system,
- assessment and management of the process of ensuring the security of the system and the data processed in it, including personal data,
- administration of servers and security devices,
- management of user rights,
- administration / management of a computer network,
- administration / management of computer hardware and software installed on it
-

9. Who is the Patient

A patient is a person applying for health services or using health services provided by an entity providing health services or a person practicing a medical profession.

10. Data protection principles

If you process data, you have to do so according to seven protection and accountability principles:

1. **Lawfulness, fairness and transparency** — Processing must be lawful, fair, and transparent to the data subject.
2. **Purpose limitation** — You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
3. **Data minimization** — You should collect and process only as much data as absolutely necessary for the purposes specified.
4. **Accuracy** — You must keep personal data accurate and up to date.
5. **Storage limitation** — You may only store personally identifying data for as long as necessary for the specified purpose.
6. **Integrity and confidentiality** — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
7. **Accountability** — The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

11. When you are allowed to process data

Article 6 of GDPR lists the instances in which it's legal to process personal data. If you want to process somebody's personal data you have to justify it with one of the following:

1. The data subject gave you specific, **unambiguous consent** to process the data.
2. Processing is necessary to execute or to prepare **to enter into a contract** to which the data subject is a party.
3. You need to process it **to comply with a legal obligation** of yours.
4. You need to process the data **to save somebody's life**.
5. Processing is necessary **to perform a task in the public interest** or to carry out some official function.
6. You have a **legitimate interest** to process someone's personal data. This is the most flexible lawful basis, though the "fundamental rights and freedoms of the data subject" always override your interests, especially if it's a child's data.

Once you've determined the lawful basis for your data processing, you need to document this basis and notify the data subject (transparency). And if you decide later to change your justification, you need to have a good reason, document this reason, and notify the data subject.

The legal basis for the processing of patients'personal data for health purposes by the Hospital is directly art. 9 sec. 2 lit. h) GDPR in connection with the provisions of national law.

The wording of Art. 9 sec. 2 lit. h) GDPR:

"Processing is necessary for the purposes of preventive healthcare or occupational medicine, for the assessment of the employee's ability to work, for medical diagnosis, and for the provision of healthcare or social security, treatment or the management of health or social care systems and services on the basis of Union or Member State law. "

12. What security principles result from data protection policies

The security rules resulting from the data protection policies at the Hospital include:

- **the principle of a closed room**

When leaving the place of classes, make sure that the room (room) has been closed, if we are the last person to leave the room.
In the absence of employees, the doors to the rooms are always locked with a key, which remains under the supervision of the employee or is returned to the reception desk.

It is unacceptable to leave the rooms unattended or lend the keys to the rooms to unauthorized persons

- **the principle of a clean desk**

Only documents or other data carriers that are necessary for the current work at a given time should be on the desk. Documentation and data carriers that are not used for current work should be secured against unauthorized access (they should be stored in locked office furniture or metal cabinets, etc.).

- **clean screen principle**

Before leaving the workplace, access to the computer should be blocked, and after finishing work, the computer should be turned off.
During operation, the computer monitor should be positioned so that it does not allow viewing of the displayed content by unauthorized persons.

- **the principle of a clean basket**

It is forbidden to throw paper documents or other media containing personal data into the trash.
All unnecessary documents (printouts, copies, drafts, etc.) must be immediately shredded in a shredder in a way that makes them unreadable.

- **the principle of a clean board**

After completing the classes or meetings, clear / secure all materials and clean the boards.

13. Breach of personal data protection, what does it mean

Breach of personal data protection means a breach of security leading to accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise processed.

The breach of confidentiality consists in the disclosure of personal data to an unauthorized person.

The breach of availability consists in the temporary or permanent loss or destruction of personal data.

The breach of integrity consists in changing the content of personal data in an unauthorized way.

Examples of violations include:

- **Providing access to medical documentation by unauthorized persons**

It is forbidden to access the medical records of the Hospital'spatients by persons who are not entitled to do so under applicable law.

- **To make medical records or health information available to individuals unauthorized**

It is forbidden to disclose medical records and information about patients (personal data of patients) to unauthorized persons and entities, contrary to the Act on Patient Rights and Patient's Rights Ombudsman.

- **Leaving documents containing personal data, including medical records, in places without supervision**

Documents containing personal data of patients should be secured in a way that prevents access to these data by unauthorized persons.
Documents that we do not currently use should be stored in closed cabinets, desks,

etc., the principle of "clean desk" applies.

- **Throwing documents containing personal data into the trash**

It is forbidden to remove paper documents containing personal data by throwing these documents into the trash.

All unnecessary documents (printouts, copies, drafts, etc.) must be immediately shredded in a way that makes them unreadable, in accordance with the applicable "clean trash" principle.

- **Providing an identifier and password to the IT system to another person**

You must not share IDs and passwords to the IT system with other people, including other employees or students / apprentices.

It is forbidden to use the Hospital's IT system if we do not have the appropriate authorization to do so. It is forbidden to use accounts belonging to other users.

- **Taking the medical documentation by the Student / Apprentice outside the Hospital**

Students / Apprentices are forbidden to remove documents belonging to the Hospital, including medical documentation / documents containing personal data (originals, copies, electronic versions) or their transmission by electronic means.

- **Using an ID and password for another person'sinformation system**

It is forbidden to use the Hospital's IT system if we do not have the appropriate authorization to do so. It is forbidden to use accounts belonging to other users.

- **Saving data on private media**

It is forbidden to save and store personal data of patients

on private media (e.g. flash drives, CDs, external drives).

- **Physical damage (fire, flooding, destruction of documents / media or devices)**

- **Theft of documents, carriers, computer hardware, devices**

14. What to do in the event of a suspected / found personal data breach?

In the event of a suspicion / finding of a breach of personal data protection, one should:

- immediately report to the Data Protection Officer any suspicion / finding of a breach personal data protection.

Contact details of the Data Protection Officer at the Hospital

e-mail address: iod@usk.wroc.pl; direct phone number (71) 733 17 97,

- also immediately notify the group leader

- refrain from any actions that may make it difficult to establish the circumstances of the violation, however, e.g. in the case of finding unsecured documents on the premises of the Hospital, containing personal data, including medical documentation, as well as its copies, printouts, etc., they should be secured so that the information contained in documentation was not disclosed to unauthorized persons.
- cooperate with the DPO in order to clarify all circumstances of the personal data breach

15. Criminal liability for breach of data protection regulations personal

The provisions on criminal liability for violation of the provisions on the protection of personal data apply to all persons involved in the processing of personal data (illegal processing of personal data).

The wording of Art. 107 paragraph. 1 and 2 of the Act of May 10, 2018 on the protection of personal data:

"1. Whoever processes personal data, although their processing is not allowed or is not authorized to process them, is subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to two years.

2. If the act specified in par. 1 concerns data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed in order to uniquely identify a natural person, data concerning health, sexuality or sexual orientation, shall be subject to a fine, the penalty of restriction of liberty or

imprisonment for up to three years ".

Persons violating the rules of personal data security, including Students / Apprentices may be subject to criminal sanctions under the provisions on the protection of personal data. Persons who are not employees of the Hospital, including Students / Apprentices, are liable towards the Hospital for damages pursuant to the provisions of the Civil Code.

16. Basic duties of Students / Apprentices

Students / Apprentices conducting classes at the Hospital are required to wear identifiers in a visible place containing at least: name and surname, name of the university and the field of study.

Students / apprentices may stay in the rooms where personal data are processed only in the presence of the Hospital Staff.

Students / apprentices are obliged in particular to familiarize themselves with:

- generally applicable legal provisions on the protection of personal data, in particular with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/45 / EC (general regulation on the protection of personal data) and the Act of May 10, 2018 on the protection of personal data;

- the Hospital's internal regulations indicated by the group's guardian, in particular in the field of personal data protection, medical documentation and information security

Students / trainees are obliged in particular to comply with the rules of personal data protection in force in the Hospital, resulting from the provisions of law and internal regulations, including:

- to exercise due diligence in order to protect personal data;

- ensuring the security of personal data processing, in particular by protecting them against unauthorized access, unjustified modification or destruction, illegal disclosure or acquisition, including the use of the required technical and organizational measures to ensure the protection of personal data;

- keep confidential the personal data obtained in connection with participation in classes at the Hospital (regardless of the method of obtaining them - written,

electronic, oral), both during the classes and after their completion.
The obligation to maintain the confidentiality of patient data also applies after the patient's death;

- counteracting breaches of personal data protection and reporting cases breach or suspected breach of data protection.

Students / Apprentices are required to comply with the law, internal regulations as well as orders and messages issued by the Director of the Hospital regarding the protection of personal data, including data contained in medical records.

17. Who can the medical records be shared with

The medical documentation is made available by the entity providing health services:

- the patient;
- the patient's statutory representative;
- a person authorized by the patient.

In addition to the patient and persons having his / her authorization, the right to access the documentation may also be obtained by other persons or entities, if their authorization results directly from the provisions of laws.

Art. 26 of the Act of November 6, 2008 on the rights of patients and the Patient's Rights Ombudsman enumerates the group of entitled persons to whom the entity providing health services may disclose the patient's medical documentation.

Medical records may, under special conditions, be made available to:

- teaching purposes;
- scientific purposes.

18. Providing medical documentation for teaching purposes

Medical documentation of entities providing health services participating in the preparation of persons for the medical profession and training of persons practicing a medical profession is made available to these persons only to the extent necessary for the implementation of didactic purposes.

[Legal basis - art. 26 sec. 3a of the Act of November 6, 2008 on patient'srights and the Patient'sRights Ombudsman]

These persons are obliged to keep the information contained in the medical records confidential, also after the patient's death**.**

[Legal basis - art. 26 sec. 3b of the Act of November 6, 2008 on patient's rights and the Patient's Rights Ombudsman]

19. Providing medical records for research purposes

Medical documentation for scientific purposes is made available to universities or research institutes, upon their request, after approval by the Director of the Hospital.

The documentation should be made available without disclosing the name and other data enabling the identification of the person **concerned.**
[Legal basis - art. 26 sec. 4 of the Act of November 6, 2008 on patient's rights and the Patient's Rights Ombudsman]

Students / Apprentices are not authorized (entitled) to provide information about the health of patients and share medical records.

20. Source materials

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/45 / EC (general regulation on the protection of personal data).
2. Act of 10 May 2018 on the protection of personal data.
3. Act of April 15, 2011 on medical activities.
4. The Act of November 6, 2008 on the rights of patients and the Patient's Rights Ombudsman .
5. Regulation of the Minister of Health of 6 April 2020 on the types, scope and templates of medical documentation and the method of its processing.
6. Code of conduct for medical branch.
7. Information Security Policy of the Hospital.
8. Personal Data Protection Policy of the Hospital