

Instructions on the obligation to observe confidentiality for students at Ulm University Hospital

Dear Student,

As part of your training at the University Hospital, you will get to know information and data about patients and other persons.

Doctors and their staff, assistants and persons in training with these persons are legally obliged to keep silent about what patients entrust to them. **§ 203 (1) of the German Criminal Code (Strafgesetzbuch, StGB)** stipulates that anyone who unauthorisedly discloses another person's secret, namely a secret belonging to the personal sphere of life or a trade or business secret entrusted to him or her or otherwise becoming known to him or her as a medical doctor or assistant, is liable to imprisonment for up to one year or a fine.

Anyone working in the Hospital who is not a doctor but who comes into contact with information about patients in the course of their duties is deemed to be an assistant to the doctor. Persons working for the doctors in preparation for the profession are treated in the same way as doctors.

The duty of confidentiality is also protected by the doctors' professional code of conduct. According to this, anyone who breaches the duty of confidentiality is acting in breach of professional law. This applies to doctors and their assistants.

In addition to these specific confidentiality regulations in the Hospital, the data confidentiality according to § 6 of the State Data Protection Act BW applies to you on account of your task. According to this, the persons performing the duties are prohibited from collecting, processing, disclosing, making accessible or otherwise using protected personal data without authorisation for a purpose other than that which is part of the respective lawful fulfilment of the duties.

Protected personal data is all material or personal information that can be attributed to identifiable persons, such as our patients, suppliers or employees. This includes classically sensitive information such as health status, but also simple information such as addresses and telephone numbers.

In accordance with legal provisions, we must oblige you to maintain confidentiality; this obligation continues even after the end of the respective activity, i.e. after you have completed your training at the Hospital. Violations of data confidentiality can be punished with imprisonment or fines in accordance with §§ 40. 41 LDSG BW and other legal provisions.

The protection of personal data extends to all personal data processed in the Hospital, regardless of the type of processing, purpose, medium or structure.

At the same time, the Data Protection Act makes it obligatory to take protective and data security measures with regard to data and procedures. Data carriers, documentation and procedures of whatever kind must be secured against unauthorised persons inside and outside the Hospital. The respective existing security regulations as well as corresponding instructions of the responsible superiors are to be observed without fail.

It is in both your and our interest that the legal obligations, the internal confidentiality regulations and the principles of proper data processing are observed, but also that any deficiencies and questions concerning data protection / data security or compliance are reported to the supervisor or the data protection officer without delay.

We would like to give you some excerpts of the most important legal provisions:

§ 203 Violation of private secrets – StGB

(1) Any person who unauthorisedly discloses another's secret, namely a secret that has been entrusted to or has otherwise become known to him or her as a

1. medical doctor, dentist, veterinary surgeon, pharmacist or member of another health profession which requires state-regulated training for the practice of the profession or the use of the professional title,
2. professional psychologists with a state-recognised scientific final examination,
3. lawyer, patent lawyer, notary public, defence counsel in proceedings governed by law, certified public accountant, sworn auditor, tax consultant, tax agent or body or member of a body of a law firm, patent law firm, auditing firm, accounting firm or tax consultancy firm,
4. marriage, family, educational or youth counsellor as well as counsellor for addiction issues in a counselling centre recognised by a public authority or corporation, institution or foundation under public law,
5. member or authorised representative of a recognised counselling centre in accordance with §§ 3 and 8 of the Pregnancy Conflict Act,
6. state-recognised social worker or state-recognised social pedagogue, or
7. member of a private client, accident or life insurance company or a private medical clearing house

shall be punished by imprisonment for up to one year or by a fine.

...

(3) Other members of a bar shall have the same status as a lawyer referred to in paragraph 1 no. 3. The aforementioned persons referred to in paragraph 1 and sentence 1 shall be deemed to have the same status as their assistants who work on a professional basis and as persons who work for them in preparation for the profession. After the death of the person obliged to maintain the secret, the persons who have obtained the secret from the deceased or from his or her estate shall also be deemed to be of equal status to the persons mentioned in paragraph 1 and sentences 1 and 2.

§ 9 Confidentiality – Professional Code of Conduct of the Medical Association BW

(1) Medical doctors must keep silent about what has been entrusted to them or become known to them in their capacity as a doctor - even after the death of the patient. This also includes written communications from patients, records of patients, X-rays and other examination findings.

(2) Doctors are authorised to disclose information if they have been released from their duty of confidentiality or if disclosure is necessary to protect a superior legal interest. Statutory obligations to make statements and reports remain unaffected. Insofar as statutory provisions restrict the doctors' duty of confidentiality, they shall inform the patients thereof.

...

§ 6 Data confidentiality– State Data Protection Act (LDSG BW)

Persons employed by public bodies are prohibited from processing or otherwise using personal data without authorisation (data confidentiality). Data confidentiality shall continue to apply even after the termination of their employment.

§ 40 Administrative offences – State Data Protection Act (LDSG BW)

(1) It is an administrative offence to

1. unauthorisedly store, use, alter, transmit or delete personal data protected by this Act
 - a) which is not in the public domain,
 - b) make such data available for retrieval by means of an automated procedure, or
 - c) retrieve or obtain data from files for himself or herself or for another person,

2. obtain by false pretences the transmission of personal data which is protected by this Act and which is not in the public domain,
3. use personal data for another purpose without the consent required under section 18 (4) sentence 3 or under section 34 (2) no. 2 or contrary to section 35 (1),
4. contrary to section 35 (2), sentence 3, combine the features referred to in section 35 (2), sentence 2, with the individual details, or
5. contrary to section 18 (5), fail to comply with an enforceable condition, or fail to comply with it in time or in full.

(2) The administrative offence may be punished with a fine of 25,000 euros.

(3) The administrative authorities within the meaning of section 36 (1) no. 1 of the Administrative Offences Act are the regional councils ("Regierungspräsidien").

§ 41 Criminal offences – State Data Protection Act (LDSG BW)

Any person who commits one of the acts specified in section 40 (1) nos. 1 to 4 in return for payment or with the intention of enriching themselves or another person or of harming another person shall be liable to imprisonment for up to two years or to a fine. The attempt is punishable.

Definitions regarding the data protection laws

- **Purpose of the law:** Everyone should be protected from being disadvantaged or adversely affected by the handling of their personal data.
- **Personal data:** are individual details about personal or material circumstances of a specific or identifiable natural person (data subject).
e.g. personal circumstances = family details, education, illnesses; material circumstances = income, property, debts, turnover
- **Special types of personal data:** Information on racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life.
- **Data subject:** A natural person about whom information on personal or material circumstances is stored.
- **Responsible body:** Any person or body that collects, processes or uses personal data on their own behalf or has others do so on their behalf.
- **Recipient:** Any person or body receiving data.
- **Third party:** Any person or body other than the responsible body. Third parties are not the data subject or persons and bodies who collect, process or use personal data on behalf of others.
- **Collection:** Obtaining data about the data subject.
- **Processing:** Storage, alteration, transmission, blocking and deletion of personal data, irrespective of the procedures used for this purpose.
- **Storage:** Gathering, recording or storing personal data on a data carrier for the purpose of further processing or use.
- **Alteration:** Rearranging the content of stored personal data.
- **Transmission:** Communicating stored personal data or personal data obtained through data processing to a third party by passing it on, by having the third party inspect it or by making it available for retrieval.
- **Blocking:** Marking stored data to restrict its further processing or use.
- **Deletion:** Making stored personal data unrecognisable.
- **Use:** Any use of personal data other than processing.
- **Anonymisation:** The data is changed in such a way that the individual details about personal or material circumstances can no longer be assigned to a natural person or can only be assigned to a natural person with a disproportionately large effort.
- **Pseudonymisation:** Replacing the name and other identifying characteristics with a marker for the purpose of excluding the identification of the data subject.