

Medical confidentiality

Ethical foundations and legal liability

Practical Class 3 · Social Medicine and Medical Ethics I · 2026/2027

Chief Assistant Professor Kostadin Kostadinov, MD, PhD

Department of Social Medicine and Public Health

Five questions about entrusted information

1. Concept and ethical foundations
2. Scope and legal framework
3. Permitted disclosure
4. Breaches and digital confidentiality
5. The physician's legal liability

Concept and ethical foundations

Three related but distinct concepts

Medical secrecy

Information about the patient learned during or in connection with healthcare.

Confidentiality

The duty not to disclose or use that information beyond its permitted purpose.

Data protection

Rules for the whole life cycle: collection, access, sharing, storage, deletion.

Confidentiality is the patient's right and the professional's duty, not the doctor's privilege.

Why we keep confidences

Autonomy

The patient decides who may access information about their health.

Non-maleficence

Shame, family conflict, job loss, discrimination, stigma.

Trust

The patient lets the doctor into their private sphere for one purpose: care.

Public health

Fear of disclosure delays testing and treatment.

Scope and legal framework

What it covers and whom it binds

Health information (Health Act, Art. 27)

- Personal data on health status and on physical and mental development.
- Prescriptions, reports, certificates and all medical records.
- Also the fact of a visit, images and samples.

Who is bound (Health Act, Art. 28c)

- Healthcare professionals and staff of healthcare establishments.
- The whole team: nurses, laboratory staff, administrators, students.
- Access follows involvement in care, not job title.

Code of Professional Ethics for Physicians

Article	Content
Art. 51	What the patient shared, what examination revealed, and everything learned in practice; kept from the family and after death.
Art. 52	Covers records, illustrative material and consultations.
Art. 53	Treating doctors are released from secrecy among themselves, unless the patient has a reasoned objection.
Art. 54	Research and teaching use only with guaranteed anonymity.
Art. 55	Reporting to institutions where the law requires it.

Levels of regulation

Level	Main subject
Hippocratic Oath, Declaration of Geneva	The moral duty
Code of Professional Ethics	The profession's standard
Health Act	Health information, access, prohibition on disclosure
Regulation (EU) 2016/679 and the Personal Data Protection Act	Health data as a special category of personal data
Penal Code, Labour Code, Obligations and Contracts Act, Professional Organisations Act	Consequences of a breach
Special legislation	Reporting duties: communicable diseases, child protection

Permitted disclosure

Health Act, Art. 28: disclosure to third parties

- Treatment continues in another healthcare establishment.
- **A threat to the health or life of others.**
- Identifying a body or the cause of death.
- State health control against epidemics.
- Medical expertise and social insurance.
- Statistics and research after identifying data are removed.
- Ministry of Health, national health bodies, NHIF, regional inspectorates, statistics institute; specified insurers.

Where others are threatened, the patient is notified before disclosure (para. 2).

The minimum-necessary rule

1

Who is the recipient?

2

On what basis?

3

Exactly which
details?

4

Through which
secure channel?

The legal basis defines the scope, the recipient and the use of the information.

If any answer is unclear, stop the disclosure until it is checked.

Relatives, the deceased and children

Relatives

Third parties unless the patient has authorised someone in writing (Health Act, Art. 28b(2)).

After death

Heirs and relatives up to the fourth degree may access the records (Health Act, Art. 28b(3)).

Child at risk

Duty to report immediately, even when bound by professional secrecy (Child Protection Act, Art. 7(2)).

Never promise an adolescent absolute secrecy.

Case 1 · The partner does not know

A patient with a recently diagnosed sexually transmitted infection refuses to tell his partner. He continues unprotected intercourse. The partner is registered with the same general practitioner.

- Which steps come before any disclosure?
- Which Health Act basis applies, and on what condition?
- Who is not a legitimate recipient?

Breaches and digital confidentiality

Teaching scale of breaches

Degree	Nature	Example
Zero	Lawful sharing for care	The treating doctor passes results to a consultant
First	Careless, low identifiability	An unnamed case discussed in the wrong place
Second	Unauthorised recipient or access without need	Staff member opens an acquaintance's record
Third	Deliberate, public or large-scale	Photo and details on social media

Lack of intent does not remove the breach.

Digital risks and data breaches

Risks

- Shared logins, unlocked screens.
- Personal messaging apps and email.
- Photos of wounds or screens.
- External artificial-intelligence tools.

After a breach

- Contain the incident.
- Report it at once through internal channels.
- Assess the data and the people affected.
- Notify the supervisory authority and the patient when required.

Every opening of a record must be traceable.

The physician's legal liability

One act, several kinds of liability

Type	Legal basis	Who enforces it
Professional	Professional Organisations Act, Arts. 37–42; Code, Arts. 51–55	Ethics committee of the regional college of the Bulgarian Medical Association
Disciplinary	Labour Code, Arts. 186–190	The employer
Administrative	Health Act, Arts. 221, 229; data protection law	Inspection bodies; data protection commission
Civil	Obligations and Contracts Act, Arts. 45, 49, 52	Court, on the victim's claim
Criminal	Penal Code, Art. 145	Court, on the victim's complaint

Professional and employment liability

Professional body

Breach of the Code (Professional Organisations Act, Art. 37(1)(1)). Penalties under Art. 38: reprimand; fine of one to five minimum monthly wages; removal from the register for 3 months to 1 year.

Employment (Labour Code)

Culpable failure to perform work duties (Arts. 186, 187(1)(10)). Penalties under Art. 188: reprimand, warning of dismissal, dismissal.

A professional-body penalty does not exclude criminal, civil or disciplinary liability (Art. 42(1)).

Administrative liability

Health Act

A fine for breaching the Act, including the prohibition in Art. 28c (Art. 229). A fine or pecuniary sanction for an establishment that violates patients' rights (Art. 221).

Data protection

Complaint to the Commission for Personal Data Protection within 6 months of learning of the breach (Personal Data Protection Act, Art. 38). Sanctions on the controller under Art. 83 of Regulation 2016/679.

The establishment is also accountable for organisation: roles, access, audit trails, training.

Civil liability

1

Unlawful disclosure

2

Harm

3

Causation

4

Fault

- Obligations and Contracts Act, Art. 45: whoever culpably causes harm must repair it; fault is presumed.
- Art. 49: whoever assigns work is liable for harm caused in performing it.
- Art. 52: non-pecuniary harm is compensated on an equitable basis.
- Personal Data Protection Act, Art. 39(2): damages for unlawful processing.

Criminal liability: Penal Code, Art. 145

“Anyone who unlawfully discloses another person’s secret that could damage someone’s good name, entrusted to them or learned in connection with their occupation...”

- Penalty: **imprisonment of up to one year or a fine.**
- The secret must threaten the good name of the person concerned.
- Prosecution on the victim’s complaint (Penal Code, Art. 161(1)).

Case 2 · A photo “for colleagues”

A resident posts a photo of a rare skin finding on social media, captioned “interesting case from yesterday”. The face is cropped, but a tattoo and the hospital wristband are visible. Acquaintances recognise the patient.

- Is the information anonymised?
- Which kinds of liability may arise?
- What should the department do now?

Keep, share, report

Keep

By default: from relatives, colleagues outside the team, employers, media.

Share

With the treating team and anyone the patient has authorised.

Report

When the law requires, to the designated recipient, to the minimum extent.

Every decision to disclose leaves a verifiable record of its basis.

Medical confidentiality is a promise to the patient.

The law defines when and how information may be shared.