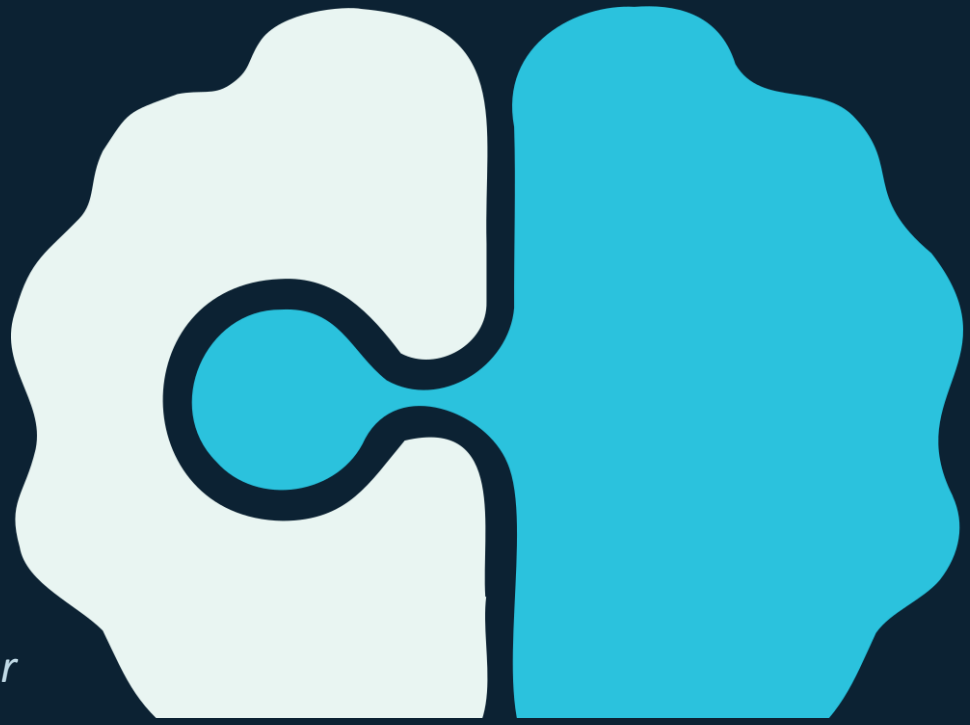
ChatMED · PERSPECTIVE

Funded by
the European Union

AI in Healthcare, Data and regulation: Why must the clinician care?



GDPR · NIS2 · AI Act · EHDS
what every clinician should understand without becoming a lawyer

ChatMED GA 101159214

Assoc. Prof. Monika Simjanoska Misheva – ChatMED Coordinator
Faculty of Computer Science & Engineering · Ss. Cyril and Methodius University, Skopje

WHERE WE START

Regulation is not somebody else's problem

Funded by the European Union

You don't need a law degree. You do need to recognise what you're standing on.

You sign the note

Every AI-assisted record carries your signature and your accountability.

You hold the data

Patient data passes through your hands.

You pick the tool

Choosing which AI to use is now a clinical decision with legal weight.

You face the patient

Consent, explanation, … these are conversations only you can have.

FOUR LAWS, ONE PRACTICE

What's already here. What's almost here.

Funded by the European Union

GDPR

Regulation (EU) 2016/679

IN FORCE since 2018

Patient data: lawful basis, purpose, minimisation, patient rights, breach reporting.

NIS2

Directive (EU) 2022/2555

IN FORCE since Oct 2024

Cybersecurity for healthcare (essential entity): risk mgmt, incident reporting, management accountability.

AI Act

Regulation (EU) 2024/1689

PHASING IN — main Aug 2026 / medical Aug 2027

Risk-based AI rules. Medical AI under MDR/IVDR is automatically high-risk.

EHDS

Regulation (EU) 2025/327

IN FORCE — main application from 2027/2029

Primary use (patient access, cross-border) and secondary use (research) of health data.

Two are already running your clinic. Two are arriving in the next 24 months. All four touch the same desk.

PART 1 · THE DATA

Three things that decide what AI can safely do

Funded by the European Union

Quality

Accurate, complete, coded, with units. Not free-text guesses.

Garbage in, garbage out! And now it shows up faster.

Provenance

Who collected it, where, when, under which consent.

An auditable lineage, or it cannot be trusted downstream.

Representativeness

Does the training cohort look like your patients?

A model tuned on others may quietly fail on yours.

Before you trust an output, check the input. *These three properties are not technicalities, they are the boundary of what AI can safely tell you!*

GDPR essentials every clinician should know

Funded by the European Union

Lawful basis (Art 6 + Art 9)

My Article 6 reason is [X], and my Article 9 condition is [Y].

Purpose limitation & minimisation

Collect what you need for the purpose stated, not what “might be useful later”.

Patient rights

Access, rectification, erasure (with clinical-record limits), portability, objection.

Records of processing

Your hospital must document what data flows where, including to every AI tool.

Breach notification

72 hours to the supervisory authority, affected patients informed when risk is high.

Research, exchange, reuse. What's allowed, and how

Funded by the European Union

Primary use

Treating the patient in front of you.

Standard healthcare exemption under GDPR Art 9(2)(h) — lawful, expected, documented in the medical record.

Secondary use

Research, policy, regulatory decision-making.

GDPR Art 9(2)(j) + EHDS Health Data Access Bodies. Patient opt-out applies in many cases.

Cross-border exchange

Sharing across EU Member States.

MyHealth@EU under EHDS — patient summaries, ePrescriptions by 2029; imaging, labs, discharge by 2031.

GDPR (EU) 2016/679; EHDS Regulation (EU) 2025/327 (Health Data Access Bodies, MyHealth@EU).

The EU AI Act: where medical AI lands

Funded by the European Union

Prohibited

social scoring, manipulation

High-risk

medical AI lives here

Limited (transparency)

chatbots labelled as AI

Minimal

spam filters, games

Risk-based pyramid

Medical AI under MDR/IVDR with a notified body is automatically high-risk.

The classification is not optional.

Provider duties

Risk mgmt, data governance, technical documentation (Annex IV), transparency, human oversight, robustness, post-market monitoring.

Deployer duties (that's you)

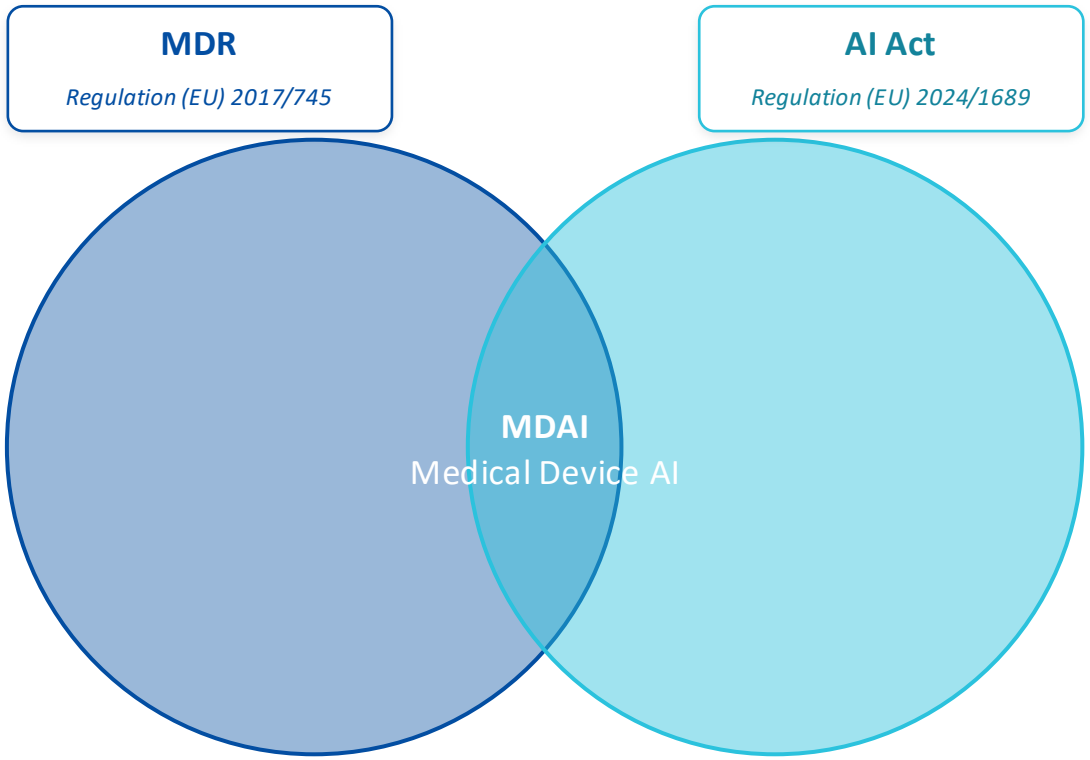
Use as intended, ensure human oversight, log usage, monitor outcomes, report incidents.

Timeline

AI literacy (Art 4) and prohibitions already in force. Main Annex III obligations: 2 Aug 2026. Medical devices (Art 6(1)): 2 Aug 2027.

Regulation (EU) 2024/1689 (AI Act); MDCG 2025-6 on Medical Device AI.

When AI becomes a medical device



One device. Two regulatory paths. One notified body.

- AI that diagnoses, treats or monitors = software as a medical device (SaMD).
- CE marking required under MDR; AI Act conformity is bolted onto the MDR notified-body route.
- Class I (no notified body) is usually NOT high-risk — unless the use case sits in Annex III.
- Significant changes trigger re-conformity — model updates included.

MDR — Regulation (EU) 2017/745; AI Act — Regulation (EU) 2024/1689; MDCG 2025-6.

TM
Funded by the European Union

“Certified” — what doctors should actually check

Funded by the European Union

A CE mark is not a universal seal of approval. *It certifies a defined intended use. Use it outside that, and the certification stops protecting you.*

Intended use

Certified for which population, which task, which clinical context?

Risk class

MDR Class I / IIa / IIb / III — and which notified body number?

Annex IV file

Ask for the technical-documentation summary. It must exist.

Training data

Provenance and demographics — does it represent your patients?

Performance

Published metrics in your setting, not just the vendor's headline numbers.

Post-market & updates

Drift monitoring, incident reporting, re-conformity on model changes.

AI Act Art 13, 16, 17; MDR Annex II (technical documentation).

Choosing a vendor: not all AI is equal

Funded by the European Union

Seven questions every clinic should ask before signing.

1. Is the tool a medical device, and under which MDR class & notified body?
2. Show me the Annex IV technical documentation summary.
3. What was the training population, and does it look like ours?
4. What performance has been published in our use context, not just the vendor's?
5. Who runs post-market monitoring, and how is drift detected?
6. How are incidents and adverse events reported to us, and to the authorities?
7. What happens to our data, including storage, processing location, secondary use?

*If a vendor cannot answer these, **they are not selling you a medical device, they are selling you risk!***

When the AI gets it wrong: who answers?

Funded by the European Union

Manufacturer / provider

Liable for defects under the revised Product Liability Directive 2024/2853 — software, including AI, is explicitly covered.

Deployer (the hospital)

Must use as intended, ensure human oversight, log usage, report incidents — AI Act deployer duties.

Clinician

Clinical judgement, informed consent, duty of care — your signature is still your signature.

Note: the AI Liability Directive was withdrawn by the Commission in 2025. *There is no harmonised EU regime for AI-specific civil liability — it falls back on national tort law, the revised Product Liability Directive, the AI Act, and clinical malpractice rules.*

Cybersecurity is part of the package: NIS2

Funded by the European Union

Healthcare is an Annex I "essential" sector. *Hospitals, labs, pharma manufacturers, medical device makers are all in scope.*

Risk management

Policies, encryption, access control, supply-chain security, backups, business continuity.

Management accountability

Boards and CEOs are personally responsible. Cybersecurity can no longer be just "delegated to IT."

Incident reporting

24h early warning → 72h notification → 1-month final report to the national authority.

Penalties

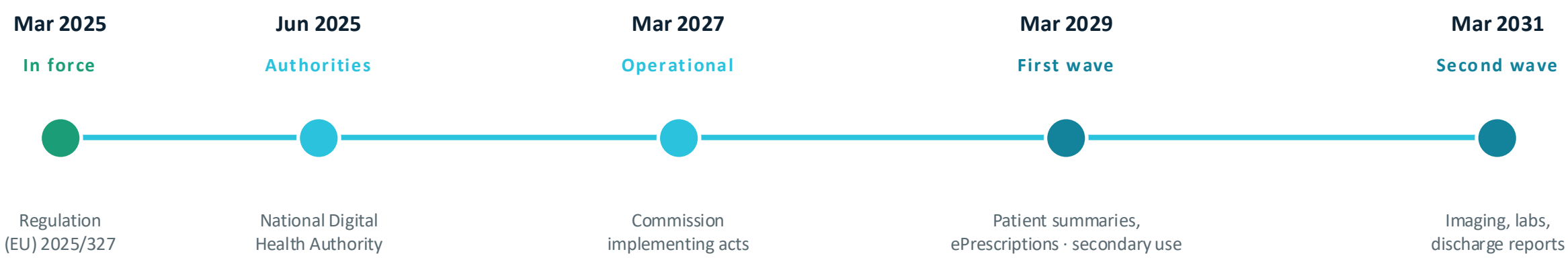
Up to €10M or 2% of worldwide annual turnover for essential entities.

NIS2 — Directive (EU) 2022/2555 (transposition deadline 17 Oct 2024).

PART 4 · WHAT'S COMING

EHDS — what's in force, what arrives by 2029

Funded by the European Union



For the clinician: *patients gain immediate access to their priority data and cross-border portability; secondary use moves to Health Data Access Bodies with patient opt-out; your records must be structured enough to travel.*

WHAT EVERY CLINICIAN MUST KNOW

Your regulation literacy minimum

Funded by the European Union

Not a law degree — a working map of the floor you're standing on.

- What patient data you may collect, why, and under which lawful basis
- Whether the AI tool in front of you is a medical device, and its class
- The intended use of that tool, and what counts as off-label
- Your role: deployer, not provider, and what each owes
- Your reporting duties: incidents, near-misses, data breaches
- What to ask a vendor before any AI enters your practice
- That AI literacy is now a legal duty under AI Act Art 4
- That the decision, and the signature stays human

AI literacy is no longer a nice-to-have. Article 4 of the AI Act makes it a duty — for staff who deploy or use AI.

BEFORE THE COUNTRY BUYS AI

What ministries owe doctors first

Funded by the European Union

Transpose NIS2 fully

Where transposition is partial, finish it. Hospitals cannot comply with a half-law.

Designate the bodies

Notified Bodies, the National Digital Health Authority (EHDS), Health Data Access Bodies.

Mandatory AI training

Article 4 of the AI Act requires literacy programmes for staff using AI in care.

Procurement standards

National rules aligning AI procurement with AI Act and MDR conformity — not vendor brochures.

Public registry

A national list of certified medical AI in clinical use, with intended use and notified body.

Incident infrastructure

One pipeline that satisfies NIS2 cyber, MDR vigilance, and AI Act post-market reporting.

Ministries do not get to skip the homework and import the tool. Doctors should refuse what the state has not yet prepared the floor for.

PART 5 · THE NEXT LAYER DOWN

Ministries can't carry this alone

The law lands on the country, but it has to be operationalised somewhere much closer to you: your own institution.

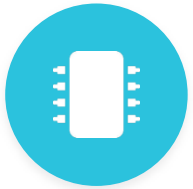
PART 5 · WHY YOU

You'll want to be in these projects

Funded by the European Union

An EU call funds AI

Horizon Europe, EU4Health, EIC — health AI is where the money and the science are.



A university builds it

Algorithms co-developed with academic partners across the consortium.

Your clinic tests it

Validated on real patients — which is exactly where you come in.

To take part, your institution — not the ministry — must lawfully hold the data, the ethics approvals, and the contracts.
No mechanisms, no seat at the table.

PART 5 · THE MISSING LAYER

What we all need: institutional mechanisms

Funded by the European Union

Data governance & a DPO

Records of processing, lawful-basis register, a named data-protection officer.

Ethics & approval pipeline

A working IRB / ethics route for AI studies — not an ad-hoc favour.

Data agreements

DPAs, joint-controller and consortium contracts ready to sign.

Secure processing environment

A controlled space where data can be analysed under EHDS / GDPR rules.

AI inventory & risk control

A register of AI tools, their class, intended use and oversight — AI Act deployer duties.

Incident & breach reporting

One workflow covering NIS2 cyber, MDR vigilance and AI Act post-market.

This is the operational floor that turns four regulations into something a clinic or faculty can actually stand on.

THE VERDICT YOU DON'T WANT

Without it, the review writes itself

Funded by the European Union

> ***"A good proposal, but insufficiently justified infrastructure to handle it."***

Strong science is not enough. If the institution can't show it can lawfully handle the data and the AI, the proposal never funds at all.

This is the sentence that quietly kills excellent ideas — not because the science was weak, but because the floor wasn't there.

PART 5 · LEARNED THE HARD WAY

ChatMED hit this wall first

Funded by the European Union

1

Faced it directly

ChatMED ran into the infrastructure-justification problem early — and saw how it stalls good science.

2

FCSE started building

The faculty began putting the institutional mechanisms in place, rather than waiting for the ministry.

3

Adapted from JSI

Days ago, FCSE's legal-department director visited the Jožef Stefan Institute to copy and re-adapt proven processes.

You don't have to invent it alone. *Mature consortium partners already have these mechanisms — borrow, adapt, and comply.*

WHAT YOU SHOULD DO

Don't give up AI. Demand the scaffolding.

Funded by the European Union

AI can genuinely revolutionise your work, walking away is the wrong response. Pushing for safe, lawful implementation is the right one.

Keep the ambition

Don't abandon AI over fear of the rules. The upside for patients is real.

Build the mechanisms

Stand up institutional governance — or partner with someone who already has it.

Make it a line-item

Put the compliance infrastructure into every proposal, explicitly and up front.

The goal isn't less AI. It's AI you can defend — to a reviewer, a regulator, and a patient.

AT LAST · THE GO / NO-GO

Are we ready to pilot the ChatMED NeuroOrchestrator?

Funded by the European Union

Defined intended use & class

What it does, for whom — and whether it is an MDR medical device.

Pilot route, not market launch

Real-world testing (AI Act Art 60) + MDR clinical investigation — not full CE yet.

Ethics approval & consent

IRB sign-off and Art 61 informed consent from participants.

Lawful data + secure space

GDPR Art 9 basis, DPAs, and a secure processing environment.

Human oversight by design

The clinician decides and signs; the NeuroOrchestrator only proposes (Art 14).

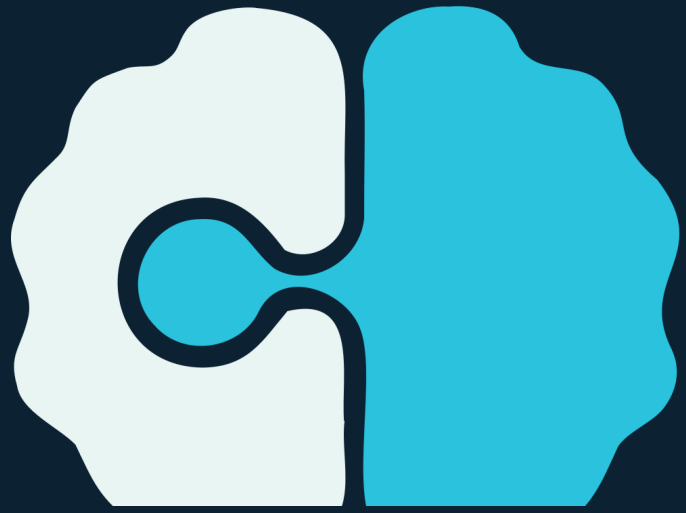
Institutional mechanisms live

Governance, DPO, incident reporting — the Part 5 scaffolding, in place.

Ready when all six are green. And a pilot's bar is lower than full deployment's — this is reachable now, not only in 2027.

ChatMED's perspective

You don't need a law degree.
You need a literate clinic.



Regulation isn't the obstacle. It's the floor you are already standing on — GDPR and NIS2 today, AI Act and EHDS tomorrow. Knowing where it holds is the difference between practising medicine with AI and being practised on.

Patient data has rules

Medical AI = medical device

Ministries do the homework

ChatMED GA 101159214

Faculty of Computer Science & Engineering · Ss. Cyril and Methodius University, Skopje

Funded by the European Union