Identomat

COMPLIANCE GUIDE

Healthcare Compliance in Latvia

COUNTRY Latvia

INDUSTRY Healthcare

LAST UPDATED 5 November 2026

KEY REGULATORS Health Inspectorate · Ministry of Health · Data State Inspectorate

Key takeaways

- Latvia has no separate licence for telehealth, and no remote-only route. Telemedicine is registered as a unit of a medical institution in the Health Inspectorate's register, and the Inspectorate will not register it without a registered office where a specialist also sees patients in person.
- Healthcare providers are not covered by Latvia's anti-money laundering (AML) law. Patient identity checks come from health law instead: patients must show a passport or identity card when asked, and pharmacies check identity before handing over prescribed medicines.
- Online, identity is checked electronically. A private telehealth service may use a qualified electronic identity (the identity card chip, eParaksts or Smart-ID) or a verification method agreed in writing with the patient, and it must accept any national electronic identity the patient offers.
- The national e-health portal accepts only qualified electronic identities, and the prescription rules in force since 2 September 2026 keep prescriptions electronic in that system, with paper only in narrow exceptions.
- EU rules on a European Health Data Space apply in stages from 26 March 2027, and from 2029 patient access services must accept any EU-recognised electronic identity; EU Digital Identity Wallets are due by 24 December 2026, and private health services that require strong online authentication must accept them by December 2027.

The Latvian market is open to private and digital healthcare providers on the same terms as clinics: registration of the medical institution and its practitioners, compliance with mandatory requirements for premises, and use of the national e-health system for prescriptions, sick-leave certificates and medical records.

The Ministry of Health sets policy, the Health Inspectorate registers and supervises providers, the National Health Service runs state-funded care, and the Data State Inspectorate enforces data protection. The national e-health system is controlled by Latvijas Digitālās veselības centrs, a company whose shares are held by the Ministry of Health.

The biggest obstacle for a digital-only entrant is that telemedicine cannot be registered on its own: it needs physical premises meeting the mandatory requirements, with an in-person specialist office. Prescribing and sick-leave workflows also run through the national e-health system, which requires a contract with the system controller and qualified increased security electronic identification for staff.

CONTENTS

1 Who regulates this sector
2 Licensing and authorisation
3 Identity framework (AML rules do not apply)
4 Identity verification and onboarding
5 Digital channels: what's different
6 Data protection and biometrics
7 Sector-specific obligations
8 Risk indicators and red flags
9 Enforcement and penalties
10 Recent changes and what to watch
11 What this means for identity verification
- Sources

1 Who regulates this sector

Authority	Remit in healthcare	Level	Official site
Ministry of Health (Veselības ministrija)	Health policy; responsible ministry for prescription and e-health regulations	National	vm.gov.lv
Health Inspectorate (Veselības inspekcija)	Medical Institutions Register; practitioner register; inspections; suspension of services; administrative penalties under the Medical Treatment Law; control of prescription circulation	National	vi.gov.lv
National Health Service (Nacionālais veselības dienests)	State-funded care contracts; prescription forms; prescription and reimbursement data	National	vmnvd.gov.lv
Latvijas Digitālās veselības centrs (state-owned company)	Controller of the national e-health system and its access rules	National	eveseliba.gov.lv
State Agency of Medicines (Zāļu valsts aģentūra)	Medicines regulation and pharmacovigilance; medical device notifications and vigilance	National	zva.gov.lv

Data State Inspectorate (Datu valsts inspekcija)	Supervisory authority under the GDPR	National	dvi.gov.lv
Supervisory Committee of Digital Security (Digitālās drošības uzraudzības komiteja)	Registers and supervises qualified electronic identification providers	National	mod.gov.lv
Financial Intelligence Unit of Latvia (Finanšu izlūkošanas dienests)	Receives suspicious-transaction reports from any person	National	fid.gov.lv
European Union	Directly applicable rules: GDPR, European Health Data Space, eIDAS	Supranational	eur-lex.europa.eu

Professional certification by the bodies named in the Medical Treatment Law is separate from registration.

2 Licensing and authorisation

Under Section 55 of the Ārstniecības likums (Medical Treatment Law), only medical institutions that meet the Cabinet's mandatory requirements may provide treatment, and Section 1 defines them as institutions registered in the Medical Institutions Register. Section 1 also defines telemedicine as remote health care using information and communication technologies, and Section 3 treats it as part of health care. There is no separate authorisation for remote care.

Registering the institution

Cabinet Regulation No. 491 of 9 August 2022, Ārstniecības iestāžu reģistra noteikumi (Medical Institutions Register Regulations), sets the process:

- Each site is registered in premises that meet the mandatory requirements (paragraph 8). Under Cabinet Regulation No. 60 of 20 January 2009, the building must be designed or adapted for the activity and accessible (paragraph 3), and an outpatient institution needs a waiting area, reception, consulting room and toilets (paragraph 24).

- Telemedicine is registered as a structural unit at a registered site (paragraph 15). The Health Inspectorate's guidance (updated 4 March 2026) states that it cannot be registered without a specialist's office for in-person consultations, and that a commercial website or app must be registered with the State Revenue Service.
- The Inspectorate may check on site and decides within 10 working days of complete documents (paragraphs 13 and 14); since Regulation No. 622 (October 2026) it may register on condition that premises use or accessibility is fixed within two years (paragraph 14.[1]).

Registering practitioners

Only practitioners on the register of medical practitioners may practise independently (Section 26), and specialist practice needs a certificate (Section 29). Access to the e-health system requires a contract with its controller (Regulation No. 134, paragraph 4.[1], since 8 November 2025). Health apps that qualify as medical device software fall under Regulation (EU) 2017/745; under Cabinet Regulation No. 461 of 15 August 2023, the State Agency of Medicines handles notifications and vigilance and the Health Inspectorate market surveillance (paragraphs 4, 18 and 19). Unregistered treatment is an offence (Section 83), and the Inspectorate may suspend non-compliant services (Sections 74 and 75).

3 Identity framework (AML rules do not apply)

Healthcare providers are not among the obliged entities listed in Section 3 of the Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likums (Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing), version in force from 15 October 2026. Two provisions still reach them:

Cash of EUR 10,000 or more

Section 3(1)(9) covers any person providing services where payment of EUR 10,000 or more is made in cash, as one operation or several linked ones. A clinic accepting such cash payments falls within the law.

Suspicious transactions

Section 3.[1] requires persons outside the Section 3 list to report every suspicious transaction to the Financial Intelligence Unit, with the same legal protection as obliged entities.

AML customer due diligence therefore does not apply to ordinary patient relationships. Identity is governed instead by health and identity law:

- **Pacientu tiesību likums (Patient Rights Law), Section 15(4):** the patient shows an identity document when a practitioner asks, except in emergencies, when it is shown as soon as possible.
- **Personu apliecinošu dokumentu likums (Personal Identification Documents Law), Section 4:** the identity documents are the identity card and the passport; the Health Inspectorate (25 November 2025) confirms a driving licence is not one.
- **Cabinet Regulation No. 512 of 25 August 2026 (prescriptions), paragraph 59** and **Cabinet Regulation No. 134 of 11 March 2014 (e-health system), paragraphs 13 and 31:** identity checks at the pharmacy and qualified electronic identification for e-health access.

4 Identity verification and onboarding

Documents and identifiers

In person, the patient shows an identity card or passport. Records and prescriptions are keyed to the personal code; Annex 3 of Regulation No. 512 requires the full name, personal code and, if the code does not contain it, the date of birth. Visiting EU, EEA or Swiss patients treated under an E or S form are identified by the form's number.

Electronic identification

The Fizisko personu elektroniskās identifikācijas likums (Law on Electronic Identification of Natural Persons), Section 3(3), treats electronic identification as equivalent to checking an identity document in person in three cases:

- identification with a qualified or qualified increased security electronic identification means;
- a method agreed in writing between the identification provider and the service provider;
- a method agreed in writing between the service provider and the patient.

Under Section 19(1.^{1}) a service provider must let users identify with any national electronic identification means, subject to technical interoperability, and under Section 19(1.^{2}) it may add further identity checks. A written agreement may not restrict the use of national means (Section 3(4)). Qualified means are issued only after an in-person identity check (Section 5(2)). The Supervisory Committee of Digital Security's register lists the eID card, eParaksts card, eParaksts card+ and eParaksts mobile as qualified increased security

means, and Smart-ID as a qualified means. Biometric matching against a document is therefore a lawful option under the second and third routes, provided the data protection conditions in section 6 are met.

Minors and representatives

Under Section 13 of the Patient Rights Law, treatment of a child under 14 needs the legal representative's informed consent; from 14 the patient consents, subject to the doctor's assessment of maturity. In the e-health system, a patient may act for their minor children and for persons who have authorised them; a patient who cannot use electronic identification can authorise a representative in person at the system controller with an identity document, or by post with a notarised power of attorney (Regulation No. 134, paragraph 32.[2]).

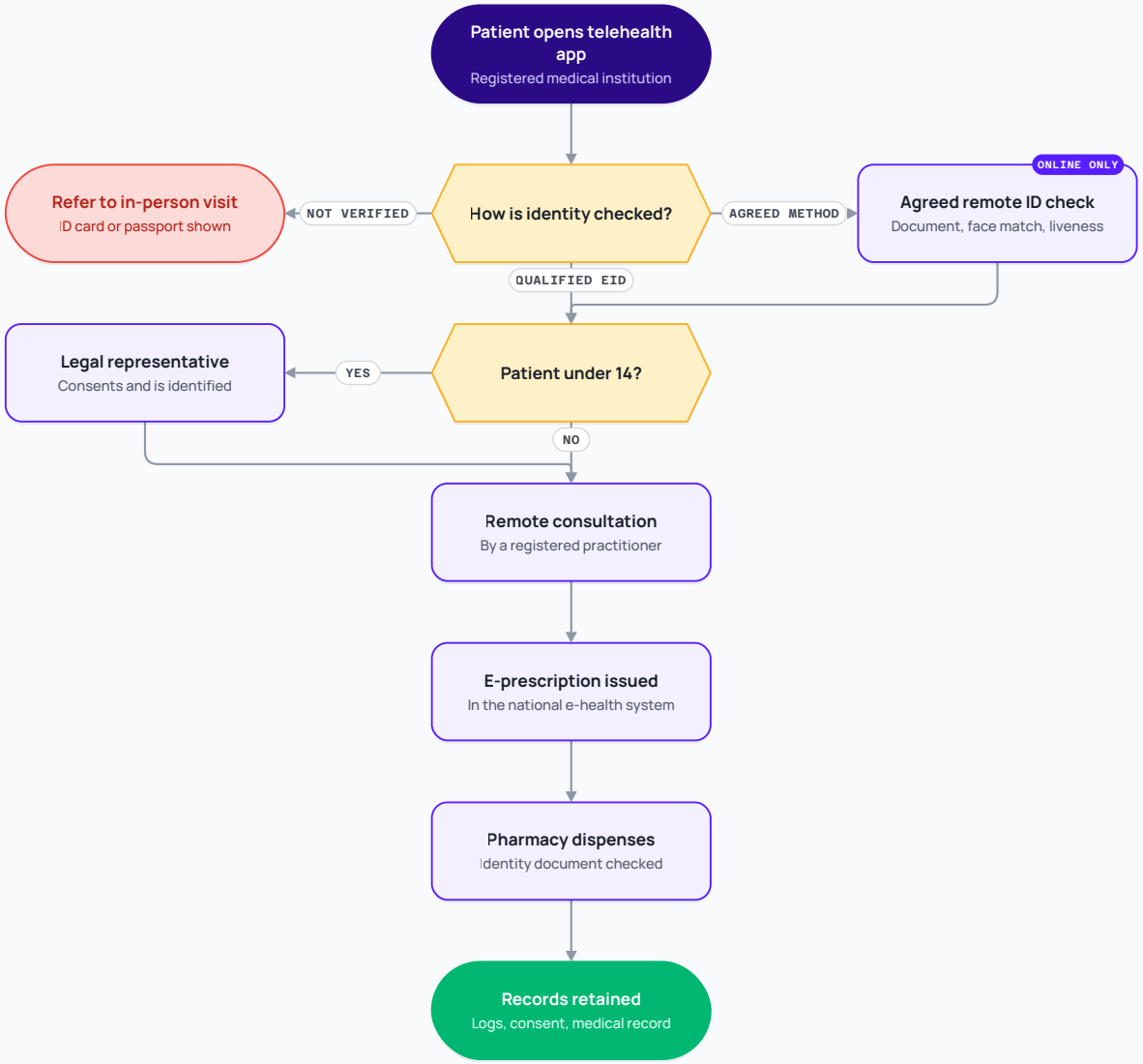


Figure 1. Remote patient onboarding and e-prescription for a registered Latvian telehealth provider.

5 Digital channels: what's different

Bottom line: telemedicine must sit inside a registered institution with an in-person office, and prescriptions are electronic in both channels; what changes online is how identity is proved, which moves from showing a document to electronic identification under the Law on Electronic Identification of Natural Persons.

Requirement	In person	Online / remote	Difference
Who may provide care	Registered institution and practitioner	Telemedicine unit of a registered institution with an in-person office	Differs
Proof of patient identity	Identity card or passport on request	Qualified eID, or a method agreed in writing	Differs
Choice of identity means	Identity card or passport	Must accept any national eID means	Differs
Patient access to own records	At the institution, through the attending doctor	E-health portal login with qualified eID only	Differs
Authorising a representative	At the controller with ID, or notarised power of attorney	Entered online by the authenticated patient	Differs
Prescription format	Electronic by default	Electronic by default	Same
Staff access to e-health	Qualified increased security eID	Qualified increased security eID	Same
Evidence to keep	Medical records	Records, plus authentication assertions and logs when qualified eID is used	Differs

Electronic identification replaces the document check

Online, identification with a qualified means or an agreed method counts as an in-person document check (eID Law, Section 3(3)), and a provider using qualified means must keep authentication assertions and failed-attempt logs (Section 19(1)).

The e-health portal is closed to weaker logins

Since 1 January 2024, patients reach their e-health data only with a qualified electronic identification means (Regulation No. 134, paragraphs 31 and 43); the portal accepts Smart-ID, eParaksts mobile and the eID card. Institutions and pharmacies need qualified increased security means (paragraph 13): eParaksts mobile, the eParaksts card or the eID card; internet-bank login ended on 1 January 2024.

Prescriptions are digital whatever the channel

Regulation No. 512 requires prescriptions in the e-health system, with paper only for use in a country without e-prescription exchange, for a doctor's own use outside an institution, or when the system is down and the medicine is urgent (paragraph 29). Narcotic and psychotropic medicines go only on special e-prescriptions (paragraph 3.2). The regulation sets no separate rules for prescriptions issued after a remote consultation.

Pending

The European Health Data Space Regulation `Adopted, applies 26 Mar 2027` gives patients the right to identify for health data access services with any electronic identification means recognised under the eIDAS Regulation (Article 16); those services apply from 26 March 2029 (Articles 4 and 105). Under eIDAS as amended by Regulation (EU) 2024/1183 `Adopted, deadlines running`, private relying parties in health that must use strong user authentication will have to accept EU Digital Identity Wallets on the user's request within 36 months of the implementing acts that entered into force in December 2024 (Article 5f(2)). The Commission's Digital Omnibus proposal of 19 November 2025 `Proposed, in negotiation` would add a GDPR exemption for biometric identity verification where the data and means stay under the user's sole control.

6 Data protection and biometrics

The GDPR applies directly, and the Fizisko personu datu apstrādes likums (Personal Data Processing Law) designates the Data State Inspectorate as supervisory authority (Section 3). Section 25(2) of that law allows health data and biometric data used for unique identification to be processed only where a GDPR Article 9(2) condition applies or a legal act provides for it under Article 9(4). Treatment rests on Article 9(2)(h); a selfie and liveness check is a separate biometric operation that needs its own Article 9(2) condition. The Data State Inspectorate's view (5 March 2021) is that private-sector facial recognition rests on consent unless a legal act provides for it, and needs a prior impact assessment.

Health-sector rules add to the GDPR:

- **Confidentiality:** patient information may be disclosed only with the patient's written consent or in cases the Patient Rights Law lists (Section 10), including after death.
- **Access:** patients may see their records and receive extracts or copies within three working days, one copy free of charge (Section 9).
- **Patient control in e-health:** patients can block all or selected institutions or practitioners from all or selected e-health data (Regulation No. 134, paragraph 32.4).
- **Children online:** consent to information society services is valid from age 13 (Personal Data Processing Law, Section 33), but consent to treatment follows the age-14 rule in the Patient Rights Law.

Retention depends on the document: Cabinet Regulation No. 265 of 4 April 2006 (medical records) sets periods from one year to 40 years after the last entry, or 15 years after the patient's death (paragraph 35).

7 Sector-specific obligations

E-prescription handling

Regulation No. 512 replaced Regulation No. 175 of 2005 on 2 September 2026. Someone collecting medicines for another person shows their own identity document and either is authorised in the e-health system or gives the prescription number and the patient's name; the pharmacist refuses on a name mismatch and records the collector's personal code (paragraph 59). Pharmacies may not dispense if the system records the patient's death (paragraph 62). E-prescriptions are kept for one to five years depending on type (paragraph 61).

Sick-leave certificates

Sick-leave certificates are issued in the e-health system and passed to employers through the State Revenue Service (Medical Treatment Law, Section 79(3)). In the first half of 2026, complaints about them rose 36% to 297, with corrective action in 66 cases (Health Inspectorate, 4 September 2026).

Cross-border patients

For cross-border patient summaries and e-prescriptions, the Latvian e-health contact point identifies the patient by personal code and checks that access has not been blocked (Regulation No. 134, paragraphs $13.^{4}$ to $13.^{7}$).

8 Risk indicators and red flags

IDENTITY AND FRAUD INDICATORS IN LATVIAN DIGITAL HEALTHCARE

- **Unsupported sick-leave requests**: remote requests for certificates without clinical grounds, the fastest-growing complaint in 2026.
- **Third-party collection**: someone collecting medicines without e-health authorisation or the prescription number.
- **Controlled medicines**: new remote patients seeking narcotic, psychotropic or Annex 7 high-risk medicines.
- **Deceased patient**: prescription or account activity after the e-health system records a death.
- **Repeated failed logins**: failed attempts, which the eID Law requires to be logged when qualified eID is used.
- **Large cash payments**: cash of EUR 10,000 or more, which brings the provider into AML scope.

9 Enforcement and penalties

Fines under the Medical Treatment Law are set in penalty units; one unit is EUR 5 (Administratīvās atbildības likums, Administrative Liability Law, Section 16(2)). The Health Inspectorate runs the proceedings (Section 88).

Offence (Medical Treatment Law)	Natural person	Legal person
Treatment without registration (Section 83)	EUR 10 to 140	EUR 250 to 1,250
Medical opinions or health care breaches (Section 84)	Warning or up to EUR 500, optional practice ban of 6 months to 2 years	EUR 250 to 2,750
Prescription form or issuance rules (Section 86)	EUR 35 to 350	EUR 280 to 1,400
Sick-leave certificate rules (Section 87)	EUR 140 to 1,400	

Treatment without medical education (Section 82)	EUR 50 to 350

The Inspectorate also issues warnings with deadlines and may suspend services, and challenges do not suspend those decisions (Sections 74 to 77). Data protection breaches are fined by the Data State Inspectorate under GDPR Article 83: up to EUR 10 million or 2% of worldwide turnover for controller and processor obligations, and up to EUR 20 million or 4% for breaches of the processing principles and Article 9.

Recent public actions

- **Pauls Stradiņš Clinical University Hospital, 18 September 2024:** the Data State Inspectorate fined the hospital EUR 2,000 under GDPR Article 83(5)(e) for failing to answer its information requests in investigations into the handling of patient data, including staff access to health records.
- **Madona Hospital, 22 September 2025:** after a breach at an IT service provider exposed staff data, the Inspectorate reprimanded the hospital and ordered a risk assessment, an incident procedure and a compliant processing contract with the provider (GDPR Articles 5, 24, 25, 28 and 32).

10 Recent changes and what to watch

- **28 Oct 2026** `In force` Patient Rights Law amendments revise disclosure rules in Section 10; a new ground for child development data applies only from 1 July 2028 `Adopted, effective 1 Jul 2028`.
- **17 Oct 2026** `In force` Regulation No. 622 amends the Medical Institutions Register rules, allowing conditional registration with a two-year deadline to fix premises use or accessibility.
- **2 Sep 2026** `In force` Regulation No. 512 replaces the 2005 prescription rules; e-prescriptions remain the default.
- **24 Dec 2026** `Adopted, deadline approaching` Latvia must provide at least one EU Digital Identity Wallet; the State Digital Development Agency organises its rollout.
- **26 Mar 2027** `Adopted, applies 26 Mar 2027` European Health Data Space Regulation applies; patient-access rights for patient summaries and e-prescriptions apply from 26 March 2029 and for other priority data from 26 March 2031.

- **Dec 2027** `Adopted, deadline running` Private relying parties in health required to use strong user authentication must accept EU Digital Identity Wallets on request, except micro and small enterprises.
- **Pending** `Proposed, in negotiation` The EU Digital Omnibus (procedure 2025/0360(COD)) would create a GDPR exemption for biometric identity verification under the user's sole control.

11 What this means for identity verification

- **Documents:** accept the identity card and passport, not a driving licence; capture the personal code, or the E or S form number for visiting EU patients.
- **Remote methods:** offer qualified eID first and accept every national eID means; a document and biometric check is lawful as a method agreed in writing with the patient.
- **Biometrics:** obtain a separate GDPR Article 9(2) basis for face matching (consent, in the Data State Inspectorate's view), run a prior impact assessment and keep a non-biometric route.
- **Age and representatives:** route patients under 14 to a verified legal representative; record the representative's identity and authority.
- **Evidence and suppliers:** keep authentication assertions and failed-attempt logs, apply the record retention in Regulation No. 265, and sign a GDPR Article 28 contract with any verification vendor.
- **Re-verification:** re-check identity before sick-leave certificates or controlled-medicine prescriptions.

IDENTOMAT

How Identomat helps

Identomat runs identity verification, screening and monitoring for regulated businesses on one platform, with workflows you configure for each market. For the requirements in this guide, that means:

- Remote patient identity verification with ID document capture, face match and biometric liveness, run as a method agreed with the patient.
- Age verification and checks on legal representatives for patients under 14.
- Configurable re-verification steps before sensitive actions such as prescriptions or certificates, built in a no-code workflow builder.
- Audit trail of every check, with cloud, on-premises or hybrid deployment to fit health data hosting needs.

Request a meeting

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- **Ārstniecības likums (Medical Treatment Law)**, Sections 1, 3, 26, 29, 55, 74 to 80, 82 to 88, version in force from 21 October 2026, likumi.lv/ta/id/44108
- **Pacientu tiesību likums (Patient Rights Law)**, Sections 9, 10, 13, 15, version in force from 28 October 2026, likumi.lv/ta/id/203008
- **Fizisko personu elektroniskās identifikācijas likums (Law on Electronic Identification of Natural Persons)**, Sections 1, 3, 5, 19, version in force from 30 September 2026, likumi.lv/ta/id/278001
- **Personu apliecinošu dokumentu likums (Personal Identification Documents Law)**, Section 4, likumi.lv/ta/id/243484
- **Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likums (AML Law)**, Sections 3 and 3.1, version in force from 15 October 2026, likumi.lv/ta/id/178987

- **Fizisko personu datu apstrādes likums (Personal Data Processing Law)**, Sections 3, 25, 33, likumi.lv/ta/id/300099
- **Administratīvās atbildības likums (Administrative Liability Law)**, Section 16, likumi.lv/ta/id/303007
- **Cabinet Regulation No. 512 of 25 August 2026, Recepšu veidlapu un recepšu aprites noteikumi (Prescription Forms and Prescription Circulation Regulations)**, in force 2 September 2026, likumi.lv/ta/id/370627
- **Cabinet Regulation No. 134 of 11 March 2014, Noteikumi par vienoto veselības nozares elektronisko informācijas sistēmu (Regulations on the Unified Health Sector Electronic Information System)**, paragraphs 2, 4.1, 12, 13, 13.4 to 13.7, 31, 32, 43, version in force from 8 August 2026, likumi.lv/ta/id/264943
- **Cabinet Regulation No. 491 of 9 August 2022, Ārstniecības iestāžu reģistra noteikumi (Medical Institutions Register Regulations)**, paragraphs 8 to 15, as amended by Regulation No. 622 of 13 October 2026, likumi.lv/ta/id/334690
- **Cabinet Regulation No. 60 of 20 January 2009, Noteikumi par obligātajām prasībām ārstniecības iestādēm un to struktūrvienībām (Mandatory Requirements for Medical Institutions)**, paragraphs 3 and 24, version in force from 22 May 2026, likumi.lv/ta/id/187621
- **Cabinet Regulation No. 655 of 4 November 2025 amending Regulation No. 134**, in force 8 November 2025, likumi.lv/ta/id/364256
- **Cabinet Regulation No. 461 of 15 August 2023, Medicīnisko ierīču noteikumi (Medical Devices Regulations)**, paragraphs 4, 18, 19, likumi.lv/ta/id/344674
- **Cabinet Regulation No. 265 of 4 April 2006, Medicīnisko dokumentu lietvedības kārtība (Procedure for Medical Records)**, paragraph 35, likumi.lv/ta/id/132359
- **Health Inspectorate, Pacienta pienākums uzrādīt personu apliecinošu dokumentu (Patient's duty to show an identity document)**, 25 November 2025, vi.gov.lv
- **Health Inspectorate, Veselības inspekcijas statistika par 2026. gada 1. pusgadu (Statistics for the first half of 2026)**, 4 September 2026, vi.gov.lv
- **E-veselība portal, E-veselības lietošana (Using e-health)**, login methods for residents, and news item of 30 March 2026 on contact and authorised persons, eveseliba.gov.lv, eveseliba.gov.lv (30 March 2026)
- **National Health Service, Atgādina par pieslēgšanās izmaiņām E-veselībā no 1. janvāra (Reminder of e-health login changes from 1 January)**, 21 December 2023, eveseliba.gov.lv
- **Data State Inspectorate, #DVIskaidro: Biometrijas datu apstrāde mazumtirdzniecībā (Processing of biometric data in retail)**, 5 March 2021, dvi.gov.lv
- **Cabinet Regulation No. 286 of 13 April 2004, Veselības ministrijas nolikums (Ministry of Health Bylaws)**, paragraph 25.9 as amended by Regulation No. 872 of 17 December 2024, likumi.lv/ta/id/357332
- **Health Inspectorate, Ārstniecības iestāžu un personu reģistrācija: jautājumi un atbildes (Registration of medical institutions and persons: questions and answers)**, updated 4 March 2026, vi.gov.lv

- **Supervisory Committee of Digital Security, Elektroniskā identifikācija and Register of Qualified and Qualified Increased Security Electronic Identification Service Providers**, mod.gov.lv
- **Data State Inspectorate, Lēmumi (Decisions)**: decision on Pauls Stradiņš Clinical University Hospital, 18 September 2024; decision No. 2-2.2/56 on Madona Hospital, 22 September 2025, dvi.gov.lv/lv/lemumi
- **Ministry of Smart Administration and Regional Development, ES Digitālās identitātes maks (EU Digital Identity Wallet)**, updated 19 March 2026, varam.gov.lv
- **Regulation (EU) 2025/327 on the European Health Data Space**, Articles 4, 16 and 105, eur-lex.europa.eu
- **Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 (European Digital Identity Framework)**, Articles 5a and 5f, eur-lex.europa.eu
- **Commission Implementing Regulations (EU) 2024/2977 and 2024/2981**, published 4 December 2024, eur-lex.europa.eu (2024/2977), eur-lex.europa.eu (2024/2981)
- **COM(2025) 837, Proposal for a Regulation on the simplification of the digital legislative framework (Digital Omnibus)**, 19 November 2025, procedure 2025/0360(COD), eur-lex.europa.eu
- **Regulation (EU) 2016/679 (GDPR)**, Articles 9 and 83, eur-lex.europa.eu