



Identomat

COMPLIANCE GUIDE

Healthcare Compliance in Estonia

COUNTRY **Estonia**

INDUSTRY **Healthcare**

LAST UPDATED **21 October 2026**

KEY REGULATORS **Health Board · State Agency of Medicines · Data Protection Inspectorate**

Key takeaways

- To treat patients in Estonia, including by video or phone, a company needs an activity licence (the Health Board's permit to provide health services) for each type of care it offers. There is no separate telehealth licence.
 - When care is given remotely, the healthcare provider itself is responsible for confirming who the patient is. The rules do not prescribe one method, so the provider must choose a reliable one and be able to show it worked.
 - Publicly funded remote consultations must be live (real-time), at an agreed time, with the patient's consent recorded and a clinician satisfied that remote care is suitable.
 - Prescriptions are issued electronically through the national Prescription Centre. Prescription medicines can be sold online only by a pharmacy that holds a distance-selling right from the State Agency of Medicines, and only against such an electronic prescription.
 - Healthcare is not covered by Estonia's anti-money laundering law, except where a provider takes large cash payments. Patient data rules and the national Health Information System drive identity design instead.
-

Estonia is open to digital healthcare. Remote consultations, electronic prescriptions and online pharmacies all operate within the existing licensing system rather than under special regimes, and every licensed provider must be technically able to exchange data with the national Health Information System.

The principal authorities are the Health Board (Terviseamet), which licenses and supervises providers; the State Agency of Medicines (Ravimiamet), which licenses pharmacies and online medicine sales; the Health Insurance Fund (Tervisekassa), which sets the conditions for publicly paid services; and the Data Protection Inspectorate.

For a new entrant, the main obstacle is not identity verification as such but integration: a licence requires named, registered health professionals, a place of business, and IT readiness for national health data exchange.

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	Level	Official site
Ministry of Social Affairs (Sotsiaalministeerium)	Health policy; regulations on documentation and data; co-controller of the Health Information System	National	sm.ee
Health Board (Terviseamet)	Activity licences, registration of health professionals, state supervision of providers	National	terviseamet.ee
State Agency of Medicines (Ravimiamet)	Pharmacy licences, distance-selling right for medicines, medicines supervision	National	ravimiamet.ee
Health Insurance Fund (Tervisekassa)	Payment for publicly funded care, list of health services, controller of the Prescription Centre, co-controller of the Health Information System	National	tervisekassa.ee
Data Protection Inspectorate (Andmekaitse Inspektsioon)	Supervision of personal and health data processing	National	aki.ee

Information System Authority (RIA)	Supervision of cybersecurity requirements for certain providers	National	ria.ee
European Union	Directly applicable data protection and health data rules	Supranational	eur-lex.europa.eu

Licensing is national: Estonia is a unitary state and has no regional health licensing.

2 Licensing and authorisation

Under § 40 of the Tervishoiuteenuste korraldamise seadus [Health Services Organisation Act], an activity licence (tegevusluba) is required for family physician care, emergency medical care, specialised medical care, and the independent provision of nursing, midwifery care, physiotherapy, speech therapy and psychological treatment. A licence grants the right to provide services at the place of business named in it (§ 40(3)).

The Health Board decides on an application within sixty days (§ 41(1)). Under § 42, a licence is granted only if staff, premises and equipment meet the requirements for the service and if the applicant's information technology is ready to exchange data with the Health Information System (§ 42 clause 6). The application names the health care professionals who will work for the provider. The Health Board may revoke a licence where the provider fails to comply with the requirements for health services (§ 48¹).

Remote care is provided under the same licence as in-person care: the Act does not create a separate telemedicine authorisation. For cross-border care, § 50³ provides that telemedicine is treated as provided in the EU Member State where the provider is established, so a provider established elsewhere in the EU is governed by its home state's rules when treating Estonian patients remotely.

Pharmacies are licensed separately by the State Agency of Medicines under the Ravimiseadus [Medicinal Products Act]. Online sale of medicines needs an additional distance-selling right (§ 31(5¹) and (5²)); see section 7.

3 Identity framework (AML rules do not apply)

Healthcare providers are not obliged entities under the Rahapesu ja terrorismi rahastamise tõkestamise seadus [Money Laundering and Terrorist Financing Prevention Act]. Section

2(1) lists credit and financial institutions, gambling operators, real estate intermediaries and other professions, but not providers of health services. Two cash provisions can still reach the sector: § 2(1) clause 5 covers traders who receive or make cash payments of €10,000 or more (in one payment or linked payments within a year), and § 2(3) covers non-profit associations and foundations that receive or pay more than €5,000 in cash. A provider organised as a foundation that accepts large cash payments should check these thresholds.

Outside those cases, there is no customer due diligence regime. Patient identity is governed instead by health law:

Health records

The Health Information System records each patient's personal identification code, date of birth, name and contact details (Health Services Organisation Act § 59¹(4)), so providers must link care to a verified identity.

Remote consultations

For publicly funded remote and video consultations, the provider is responsible for identifying the patient (Tervisekassa list of health services, § 9(36) clause 6).

Prescriptions

A prescription carries the patient's name, personal identification code and contact details, and the buyer of a prescription medicine must be identified at dispensing.

4

Identity verification and onboarding

Who is identified, and against what. The national identifier is the personal identification code (isikukood). Health records sent to the Health Information System are keyed to it (§ 59¹(4) clause 1), and every prescription must show the patient's name, personal identification code and contact details (prescription regulation § 4(1) clause 1). An onboarding flow that cannot establish this code reliably cannot exchange data with the national system.

Accepted methods. Health law does not list approved documents or remote methods for providers. The Tervisekassa list of health services places the duty on the provider: in a remote consultation, the provider is responsible for identifying the patient, and the technology used must comply with the Personal Data Protection Act and the GDPR (§

9(36) clauses 5 and 6). At the pharmacy counter, the regulation on prescribing and dispensing (Ravimite väljakirjutamine ja apteekidest väljastamine) requires the buyer of a prescription medicine to be identified by an identity document or by electronic identification (§ 6(1)). A person collecting a medicine for someone else must also give the patient's name and personal identification code, and the pharmacist checks in the Prescription Centre that collection by another person is allowed.

Biometrics and liveness. No health-specific rule requires or prohibits face matching or liveness detection. If used, biometric data falls under the special-category rules of the GDPR (section 6).

Representatives. The Health Information System holds data on a patient's guardian or representative (§ 59¹(4) clause 2), and the Prescription Centre receives legal representatives' data from the population register (Medicinal Products Act § 81), so flows for children and represented adults must capture who is acting.

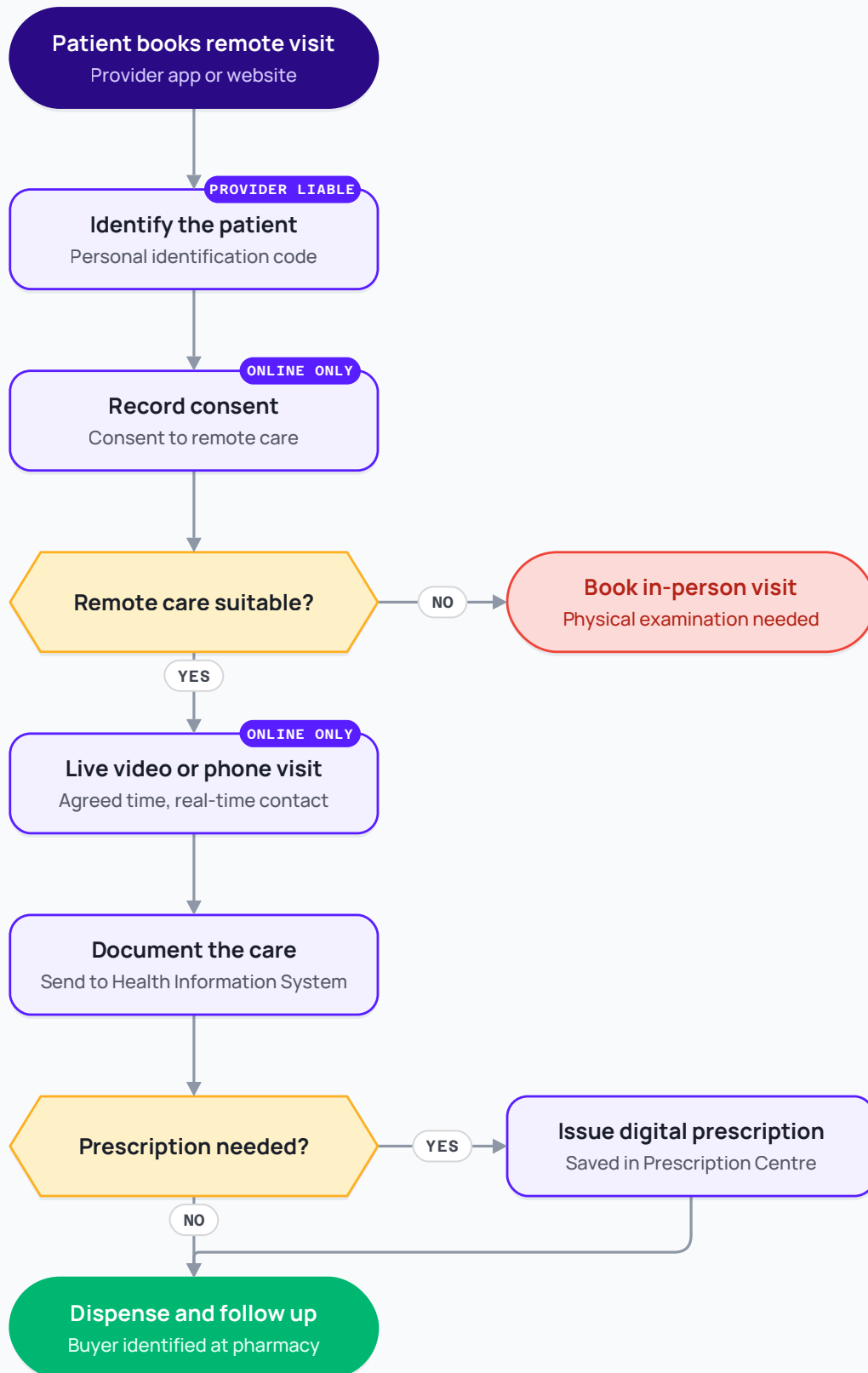


Figure 1. Remote consultation and e-prescription flow for a licensed provider in Estonia.

Bottom line: the licence, the records and the e-prescription are channel-neutral, but publicly funded remote consultations come with extra conditions (documented consent, live contact, a suitability decision and provider responsibility for identification), and online medicine sales need a separate right from the State Agency of Medicines.

Requirement	In person	Online / remote	Difference
Authorisation to provide care	Activity licence	Same activity licence; no telemedicine licence	Same
Patient identification	Provider identifies the patient	Provider expressly responsible for identification	Same
Consent to the format	Not separately documented	Consent to remote care documented	Differs
Form of contact	Face to face	Live, at an agreed time; clinician decides suitability	Differs
Prescriptions	Electronic, via Prescription Centre	Electronic, via Prescription Centre	Same
Buying prescription medicines	Paper or digital prescription; buyer identified at counter	Digital prescription only; pharmacy needs distance-selling right	Differs
Handover of medicines	At the counter	Against signature or other identity feature	Differs
Record retention	30 years for care data	30 years for care data	Same
Cross-border care	Rules of the state where care is given	Rules of the provider's state of establishment	Differs

Conditions for remote consultations

The Government's regulation on the Tervisekassa list of health services sets six conditions for remote and video consultations it pays for (§ 9(36)): quality must be maintained or improved compared with an in-person visit; the treating or referring clinician decides

whether remote care suits the problem and the provider assesses the patient's technical readiness; the patient's consent is documented; contact is synchronous at an agreed time and in an agreed way; the technology complies with data protection law; and the provider is responsible for identifying the patient. These conditions are payment conditions for publicly funded care, but they describe the standard a supervisor is likely to expect from any remote consultation.

Online pharmacies

Only a general pharmacy licence holder with a distance-selling right may sell medicines online (Medicinal Products Act § 31(5¹)). The website must display the common EU logo (§ 31(5³)), prescription medicines may be dispensed at a distance only against an electronic prescription stored in the Prescription Centre (§ 33(1³)), and the State Agency of Medicines publishes the list of authorised online pharmacies (§ 31(8)). Deliveries must be handed to the addressee or their designated representative against a signature or another feature that verifies identity (prescription regulation § 6²(7)).

Video pharmacy service

A pharmacy may provide pharmacy service by video call with a separate right from the State Agency of Medicines; without a pharmacist present, this is allowed only in a branch pharmacy in a non-urban settlement with no other pharmacy (Medicinal Products Act § 31(5⁸)).

6 Data protection and biometrics

The GDPR applies directly, supplemented by the *Isikuandmete kaitse seadus* [Personal Data Protection Act]; the Data Protection Inspectorate supervises both. For healthcare the key national rule is § 4¹ of the Health Services Organisation Act: providers bound by professional confidentiality may process personal data, including special categories, without the data subject's permission for the provision of health services and for planning care. Consent is therefore not the legal basis for clinical processing, although remote consultations still require documented consent to the remote format.

Section 4²(2¹) requires providers to ensure the traceability of personal data processing in their own information systems, which in practice means access logs. Records of outpatient and inpatient care are kept for 30 years from confirmation of the data (§ 4²(4)), with shorter periods for items such as referrals; a provider need not keep data itself once it has sent the data to the Health Information System (§ 4²(5¹)).

Patients have access to their own data in the Health Information System and may prohibit health professionals' access to it (§ 59³(1) and (3)); a provider must give effect to such a wish immediately (§ 59³(4)). The Prescription Centre has a parallel right to block providers' access (Medicinal Products Act § 81).

Biometric templates or face images captured for identification are special-category data under the GDPR. Health law gives no separate basis for them, so a provider using face matching for remote identification needs its own GDPR legal basis, a retention limit, and a clear separation from clinical records.

7 Sector-specific obligations

Reporting to the Health Information System

Providers must submit data on waiting lists, medical images and the health services they provide (§ 59²(1)). The system, co-controlled by the Ministry of Social Affairs and Tervisekassa (§ 59¹(2)), keeps most data without time limit, waiting list and digital registration data for five years, and medical images for 30 years (§ 59¹(5)). Patients may themselves forward data to the system, including through software solutions permitted by its statutes (§ 59²(1²)).

Digital prescriptions

Anyone entitled to prescribe must issue prescriptions electronically in the Prescription Centre; paper is allowed only where the Prescription Centre cannot be used for objective reasons (Medicinal Products Act § 81(7)). Pharmacies process every prescription, other than an EU prescription, through the Prescription Centre and record the buyer's data. Tervisekassa is the controller, and Prescription Centre data is kept for seven years.

Patient safety and quality

Since 1 November 2024, providers must analyse patient safety incidents and report them to the patient safety database in a form that does not directly identify the patient or professional (§ 3²(8)). Supporting documents are kept for 30 years.

Risk indicators and red flags

Healthcare is not an anti-money laundering sector in Estonia. The indicators below are identity and fraud risks that the Estonian rules on remote care and medicines are built to address.

IDENTITY-ABUSE INDICATORS IN DIGITAL HEALTHCARE

- **Mismatched identity code:** the personal identification code entered does not match the electronically identified user.
- **Proxy collection:** repeated collection of prescription medicines for other people without a recorded right in the Prescription Centre.
- **Remote-only demand for prescriptions:** a first contact that seeks a prescription without a clinical history and resists an in-person examination.
- **Unlisted online pharmacy:** a site selling medicines that is not on the State Agency of Medicines' list or lacks the common EU logo.
- **Delivery diversion:** requests to hand medicines to someone other than the addressee or a named representative.
- **Unusual record access:** staff access to patient records with no care relationship, visible in traceability logs.

Enforcement and penalties

The Health Board exercises state supervision over providers and may obtain personal data, including special-category data, for that purpose (§ 60(1)); it may apply the special supervision measures of the Law Enforcement Act (§ 61) and revoke an activity licence in whole or in part (§§ 48 to 49). From 1 April 2026, the Act's own €640 cap on non-compliance levies (§ 62) was repealed. The Information System Authority supervises the cybersecurity requirements set for certain providers (§ 60(2)).

Breach	Natural person	Legal person	Provision
Breach of medicine handling requirements (including pharmacy and distance-selling rules)	Up to 300 fine units	Up to €32,000	Medicinal Products Act § 104

Breach of prescribing requirements	Up to 200 fine units	Up to €32,000	Medicinal Products Act § 110
Breach of controller or processor duties (GDPR Articles 8, 11, 25 to 39, 42, 43), including security	Up to €10,000,000	Up to €10,000,000 or 2% of worldwide turnover	Personal Data Protection Act § 62
Breach of processing principles or consent rules (GDPR Articles 5 to 7 and 9)	Up to €20,000,000	Up to €20,000,000 or 4% of worldwide turnover	Personal Data Protection Act § 65
Breach of data subject rights (GDPR Articles 12 to 22)	Up to €20,000,000	Up to €20,000,000 or 4% of worldwide turnover	Personal Data Protection Act § 66

Estonia imposes data protection fines through misdemeanour proceedings rather than administrative fines, and each fine is set per offence up to these maxima. Separately, the Data Protection Inspectorate may impose a non-compliance levy for failure to follow its precept, up to €20,000,000 or 4% of worldwide turnover each time (Personal Data Protection Act § 60).

10 Recent changes and what to watch

- **26 March 2027** Adopted, applies from 26 Mar 2027 Regulation (EU) 2025/327 on the European Health Data Space, which governs access to and exchange of electronic health data, begins to apply; providers and health software vendors should plan system changes now.
- **1 October 2026** In force Amendments to the Health Services Organisation Act (RT I, 30.06.2026, 1) set crisis-preparedness duties for providers and the Health Board, including providers with a standing crisis task.
- **1 July 2026** In force An amended version of the Tervisekassa list of health services applies; the conditions for remote and video consultations remain in § 9(36).
- **1 April 2026** In force Amendments (RT I, 17.03.2026, 1) amended the documentation and retention rules in § 4², widened the data held in the Health Information System, allowed fees for research data access, and repealed the €640 non-compliance levy cap.
- **1 September 2025** In force The purposes of the Health Information System and the bodies entitled to receive its data were updated (RT I, 02.01.2025, 3).

Design onboarding around the personal identification code: it is the key for Health Information System submissions, prescriptions and dispensing, so the remote flow should bind a verified identity to that code before any clinical record or prescription is created. Because the provider is responsible for identification in remote care and no method is prescribed, the method chosen should be documented and its result logged, alongside the consent to remote care that publicly funded consultations require.

Electronic identification is expressly recognised at the pharmacy counter, which makes it the natural benchmark for remote flows. Document capture with face matching is not prohibited, but it brings special-category biometric processing that health law does not authorise, so it needs its own legal basis and short retention, kept apart from clinical records retained for 30 years.

Flows must handle representatives and proxies (guardians, legal representatives, people collecting medicines for others), respect patients' blocks on access, and log access for traceability. Online pharmacies need a second identity step at delivery, when the parcel is handed over against a signature or another identity feature. Cross-border providers should note that telemedicine follows the rules of their state of establishment, while Estonian prescriptions and Health Information System access still require Estonian identifiers.

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 bound to the personal identification code before a record or prescription is created.
- ID document capture and verification, including NFC chip reading, with face match and biometric liveness where a provider chooses them.
- E-signatures and KYC questionnaires to record consent to remote care alongside the identity check.
- Configurable no-code workflows with an audit trail of each check, deployable in the cloud, on-premises or hybrid.

[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

- **Tervishoiuteenuste korraldamise seadus [Health Services Organisation Act]**, consolidated text in force from 1 October 2026 (RT I, 30.06.2026, 132), §§ 3², 4¹, 4², 40 to 49, 50³, 59¹ to 59³, 60, 62, Riigi Teataja, riigiteataja.ee/akt/130062026132; English translation (version 1 September to 31 December 2025), riigiteataja.ee/en
- **Ravimiseadus [Medicinal Products Act]**, consolidated text in force from 1 October 2026, §§ 31, 33, 81, 104, 110, Riigi Teataja, riigiteataja.ee/akt/111072026037
- **Ravimite väljakirjutamine ja apteekidest väljastamine [Prescribing of medicinal products and dispensing from pharmacies]**, Minister of Social Affairs regulation, version in force from 10 July 2026, §§ 4, 6, 6², Riigi Teataja, riigiteataja.ee/akt/107072026011

- Tervisekassa tervishoiuteenuste loetelu [Tervisekassa list of health services], Government regulation No 37 of 23 March 2026, version in force from 1 July 2026, § 9(36), Riigi Teataja, riigiteataja.ee/akt/116062026020
- Rahapesu ja terrorismi rahastamise tõkestamise seadus [Money Laundering and Terrorist Financing Prevention Act], version in force from 21 July 2026, § 2, Riigi Teataja, riigiteataja.ee/akt/111072026093
- Isikuandmete kaitse seadus [Personal Data Protection Act], version in force from 1 October 2026, §§ 60, 62, 65, 66, Riigi Teataja, riigiteataja.ee/akt/130062026052
- Regulation (EU) 2025/327 on the European Health Data Space, OJ L, 2025/327, 5.3.2025, EUR-Lex, eur-lex.europa.eu/eli/2025/327/oj