Identomat

COMPLIANCE GUIDE

Healthcare Compliance in the United Kingdom

COUNTRY United Kingdom

INDUSTRY Healthcare

LAST UPDATED 16 October 2026

KEY REGULATORS Care Quality Commission · General Pharmaceutical Council · Information Commission

Key takeaways

- UK anti-money laundering (AML) rules do not cover healthcare providers. Patient identity checks are required instead by medicines law, by the pharmacy regulator and by NHS standards.
- An online clinic or doctor service treating patients in England must register with the Care Quality Commission (CQC) before it starts. Operating without registration is a criminal offence.
- Online pharmacies in Great Britain must check that each patient is who they claim to be, with a check matched to the risk of the medicine. For weight-loss and other higher-risk medicines, an online questionnaire on its own is not enough.
- For weight-loss medicines, the prescriber must independently confirm the patient's weight, height or body mass index, for example by video or from clinical records. A phone call does not count.
- Face scans used to verify identity are special category data. Explicit consent is normally the right legal condition, and patients who decline must be offered a non-biometric alternative.

The UK market is open to online healthcare, including telehealth consultations, online prescribing and internet pharmacies, but it is regulated as strictly as face-to-face care. Regulators expect the same safeguards whether the patient walks into a surgery or uses an app.

The principal regulators are the Care Quality Commission for providers in England, the General Pharmaceutical Council (GPhC) for pharmacies in Great Britain, and the Information Commission for data protection across the UK. Health regulation is devolved, so Scotland, Wales and Northern Ireland have their own service regulators.

The biggest obstacle for a new entrant is clinical rather than technical. A fast, questionnaire-only prescribing flow for higher-risk medicines does not meet current GPhC expectations, and identity checks are part of that test.

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

Regulator	Remit	Level	Official site
Care Quality Commission (CQC)	Registration and inspection of health and care providers, including online primary care	England	cqc.org.uk
General Pharmaceutical Council (GPhC)	Registration and inspection of pharmacies and pharmacy professionals, including online pharmacies	Great Britain	pharmacyregulation.org
Medicines and Healthcare products Regulatory Agency (MHRA)	Medicines and medical devices law	UK	gov.uk/mhra
NHS England	NHS login and identity standards for NHS digital services	England	england.nhs.uk
Information Commission (formerly the ICO)	Data protection, including health and biometric data	UK	ico.org.uk
Department of Health and Social Care	Health policy and medicines legislation	UK and England	gov.uk/dhsc

Outside England, independent healthcare providers register with Healthcare Improvement Scotland, Healthcare Inspectorate Wales or the Regulation and Quality Improvement Authority in Northern Ireland, which the GPhC lists as the relevant service regulators alongside the CQC. The General Medical Council regulates doctors across the UK.

2 Licensing and authorisation

In England, any person who carries on a regulated activity without being registered with the CQC commits an offence under section 10 of the Health and Social Care Act 2008. The regulated activities are listed in Schedule 1 to the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014. The CQC states that it regulates providers of online primary care in England where they deliver a regulated activity by online means, including video consultations and prescribing in response to online forms. The activities it most commonly registers for these providers are treatment of disease, disorder or injury; transport services, triage and medical advice provided remotely; and diagnostic and screening procedures. Registration is by activity, so a service that adds remote triage to treatment needs both on its registration.

Any pharmacy in Great Britain that supplies medicines, including over the internet, must be registered with the GPhC and meet its standards for registered pharmacies. A telehealth service that prescribes and then routes prescriptions to a partner pharmacy therefore usually depends on two registrations: the prescriber's with the CQC (or the devolved equivalent) and the pharmacy's with the GPhC.

Under regulation 214 of the Human Medicines Regulations 2012, a prescription only medicine may be sold or supplied only in accordance with a prescription from an appropriate practitioner, such as a doctor or an independent prescriber. These Regulations extend across the UK.

3 Identity framework (AML rules do not apply)

Healthcare providers, online clinics and pharmacies are not relevant persons under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. There is no customer due diligence regime, no suspicious activity reporting duty specific to the sector and no AML supervisor. Financial sanctions law applies to them as it does to any UK business.

Identity obligations come from three other sources instead:

Medicines law

A prescription must carry the name and address of the patient, and their age if under 12 (regulation 217). Electronic prescriptions must carry an advanced electronic signature that identifies the prescriber (regulation 219).

Regulator standards

The GPhC requires online pharmacies to confirm the patient's identity with a check appropriate to the medicine, and the CQC inspects whether online providers know who they are treating.

NHS standards

NHS services in England follow NHS England's identity verification guidance and the national identity standard for digital health and care services, delivered at scale through NHS login.

The purpose differs from financial crime law. The aim is to make sure the right patient receives the right medicine and that the clinical information supporting a prescription belongs to that patient. That makes identity a patient-safety control, assessed by clinical regulators.

4 Identity verification and onboarding

The GPhC's Guidance for registered pharmacies providing pharmacy services at a distance, including on the internet (February 2025) is the most specific statement of what a UK online health service must do. For sales and supplies of pharmacy (P) and prescription only medicines (POM), staff must be able to check that the person is who they claim to be, using an identity check appropriate to the medicine. The guidance names two example methods: an external credit reference database, and an identity-checking service using photo ID verification. Standard operating procedures may vary the method by medicine risk, or adopt the NHS identity verification and authentication standard for digital health and care services.

For higher-risk medicines supplied through an online prescribing service, the prescriber must have robust processes to check the person's identity so that medicines go to the right person. Identity is then one of four linked safeguards: the prescriber does not rely on a questionnaire alone and independently verifies what the person says; the person gives

their GP's details and consent to share information, or the prescriber records a documented risk decision if not; and prescribing follows UK national guidelines.

NHS identity routes

NHS England's guidance on identity verification for GP online services accepts three methods: two documents, one with a photo (for example a passport, photo driving licence or a bank statement from the last three months); personal vouching by a member of practice staff who knows the patient; and vouching using confirmation questions drawn from the patient record. It describes NHS login as the national platform through which patients prove their identity once and reuse it across digital health services, and requires identity verification and explicit patient consent before anyone is granted proxy access to another person's record.

Age and capacity

Under the GPhC guidance, the chosen consultation method must let the professional assess the person's capacity to make decisions about treatment, which is especially important for high-risk and mental health medicines. NHS England's guidance treats 11 as the age at which parental proxy access to a child's record should be reviewed, and 16 as the age at which a young person is usually considered able to consent.

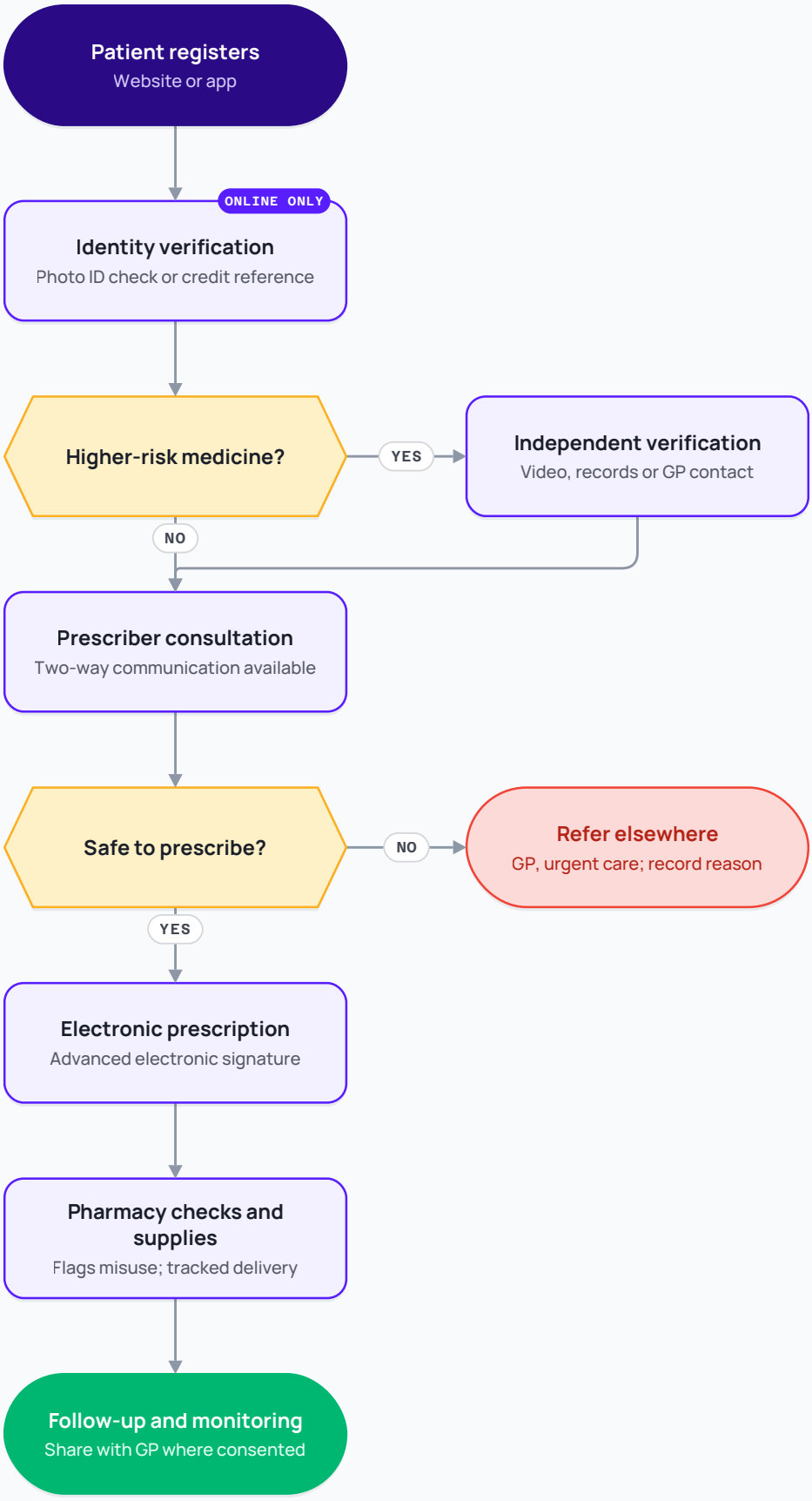


Figure 1. Online consultation and prescribing flow for a UK telehealth service with a partner pharmacy.

5 Digital channels: what's different

Bottom line: the law is channel-neutral, but regulators add online-only safeguards. Where a pharmacist or GP can see the patient in person, an online service must replace that with a documented identity check and, for higher-risk medicines, independent verification of what the patient says.

Requirement	In person	Online / remote	Difference
Registration with the CQC or GPhC	Required	Required; same regime	Same
Prescription only medicine needs a valid prescription	Required	Required	Same
Prescription signature	Signed in ink	Advanced electronic signature	Differs
Patient identity check	Professional judgement at the counter or surgery	Documented check matched to medicine risk, such as photo ID or credit reference	Differs
Weight-loss medicines	Measured in person	Independently verified by video, records or another provider; phone not acceptable	Differs
Consultation method	Face to face	Must allow timely two-way communication, or refer the patient elsewhere	Differs
Misuse detection	Staff awareness	Automated flags for multiple accounts, shared payment details and repeat orders	Differs
Biometric data	Rarely processed	Face matching is special category data; explicit consent and an alternative	Differs

Same law, extra safeguards

The GPhC states that the same laws apply whether services are provided in person, at a distance or on the internet, but that providing services at a distance, especially online, carries particular risks that must be managed. The CQC says its approach to online providers is similar to how it regulates face-to-face primary care.

No questionnaire-only prescribing for higher-risk medicines

The GPhC lists medicines that are not suitable for prescribing by a questionnaire model alone, including antimicrobials, medicines liable to misuse (such as opioids, sedatives and gabapentinoids), medicines with a higher risk of harm in overdose, medicines for long-term conditions needing monitoring, and medicines for weight management. If a prescriber chooses not to use two-way communication, they must record a justification specific to that patient.

Platform transparency

An online pharmacy's website or app must prominently display its GPhC registration number, owner and superintendent pharmacist, and, where medicines follow an online consultation, the prescriber's name, registration number and country of registration. It must not mislead patients about who is supplying or prescribing, or where they are based.

6 Data protection and biometrics

The UK GDPR and the Data Protection Act 2018 apply, as amended by the Data (Use and Access) Act 2025, whose main data protection changes took effect on 5 February 2026. Health data is special category data, and a telehealth onboarding flow typically collects both health data and identity data in the same session.

Under the regulator's biometric recognition guidance, using biometric data to identify someone makes it special category data. Explicit consent is likely to be the most appropriate condition, because no specific Article 9 condition covers identity verification. Consent must be freely given, so a service relying on it must offer a suitable non-biometric alternative, such as a document check reviewed by staff. The guidance notes that it is under review following the 2025 Act.

The GPhC adds sector expectations: personal data collected through an online pharmacy platform should be stored on servers in the UK or in a jurisdiction with equivalent protection, information security should be audited by independent experts, and clinical records must show the reasons for each decision to supply or refuse.

7 Sector-specific obligations

Electronic prescriptions

An electronic prescription for a prescription only medicine must be created in electronic form, signed with an advanced electronic signature and sent to the dispenser electronically. Prescriptions for Schedule 2 and 3 controlled drugs must travel through the NHS electronic prescription service (regulation 219). An advanced electronic signature must be uniquely linked to and capable of identifying the prescriber, which makes prescriber authentication an identity requirement in its own right.

Third-party prescribers and overseas services

The pharmacy owner and superintendent pharmacist remain responsible for the service even when part of it is subcontracted. The GPhC expects written service-level agreements with third-party prescribing services, confirmation that those services are registered with the right regulator, and active management of the extra risks of prescribers not registered with a UK regulator, including indemnity cover. Pharmacies must not work with online providers that try to avoid UK regulation.

Delivery to the right person

Delivery to a home or workplace raises the risk of medicines reaching the wrong person. The GPhC expects tracked delivery, records of consent to the delivery method and of successful delivery, and secure codes for collection lockers made available only to the right person.

Digital identity providers

Providers of digital identity checks can be certified against the statutory UK digital verification services trust framework under the Data (Use and Access) Act 2025, which took effect on 1 December 2025. Version 1.0 was published on 9 June 2026 and version 0.4 remains certifiable.

8 Risk indicators and red flags

IDENTITY AND MISUSE INDICATORS IN ONLINE HEALTHCARE (GPHC AND CQC)

- **Multiple accounts**: one person using several accounts to place orders.
- **Shared payment details**: orders that appear to come from different people but use the same card.
- **Address clustering**: multiple orders sent to the same address.
- **Excessive requests**: quantities that are too large or orders placed too often.
- **Risky combinations**: inappropriate combinations of medicines, or repeated requests for infection treatments.
- **Unverifiable history**: no GP details or no consent to contact a GP for a higher-risk medicine.
- **Duress or coercion**: signs that someone is being pressured into obtaining a medicine, or into granting proxy access to records.

9 Enforcement and penalties

Unregistered activity (England). Carrying on a regulated activity without CQC registration is a criminal offence. On summary conviction it carries a fine or imprisonment up to the general limit in a magistrates' court; on indictment, a fine, up to 12 months' imprisonment, or both (section 10(4)). The CQC can also suspend registrations, impose conditions and issue warning notices. Its inspections of online primary care providers have led to suspensions and conditions where it found insufficient checks on patient identity, including a requirement notice ordering one provider to put in place a robust system to verify patient identity (CQC announcement).

Pharmacies (Great Britain). Any pharmacy that fails a standard must complete an improvement action plan within 10, 20 or 60 working days, published alongside its inspection report. Where there is a serious risk to patient safety, the GPhC can use statutory powers, including improvement notices and conditions on the registered premises (GPhC inspection outcomes). Failing to meet the standards can lead to action against the pharmacy, the owner and the superintendent pharmacist, and to fitness to practise investigations of the professionals involved.

Data protection (UK). Fines for the most serious infringements reach the higher of £17,500,000 or 4% of total annual worldwide turnover; other infringements carry a

standard maximum of the higher of £8,700,000 or 2% (Data Protection Act 2018, section 157). In March 2025 the regulator fined Advanced Computer Software Group, an IT supplier to the NHS, £3.07m after attackers entered its health and care systems through a customer account without multi-factor authentication (enforcement notice).

10 Recent changes and what to watch

- **30 September 2026** `In force` The Information Commission replaced the Information Commissioner's Office as the data protection regulator. Existing guidance and enforcement continue under the new body.
- **9 June 2026** `In force` Version 1.0 of the UK digital verification services trust framework was published; version 0.4 remains certifiable. Check which version an identity provider is certified against.
- **19 June 2026** `In force` Organisations must have a process for handling data protection complaints, under a duty added by the Data (Use and Access) Act 2025.
- **5 February 2026** `In force` The main data protection changes in the 2025 Act took effect, including new rules on automated decision-making and subject access timelines. Biometric guidance remains under review.
- **1 December 2025** `In force` The digital verification services trust framework and register became statutory, giving certified identity providers a legal footing.
- **February 2025** `In force` The GPhC's updated distance-selling guidance added weight-loss medicines to the higher-risk list and ended questionnaire-only prescribing for those medicines.

11 What this means for identity verification

Tier checks by medicine risk. The rules expect a check appropriate to the medicine, so a single fixed flow is rarely right. A credit reference check may suit low-risk supplies, while higher-risk medicines call for photo ID verification against the person and independent verification of clinical information.

Pair identity with clinical evidence. For weight-loss medicines, the same session that verifies identity often also needs to capture independent evidence of weight or height, for example by video. Phone-only checks are not acceptable for that purpose.

Plan for devolution. A UK-wide service deals with the CQC in England and separate regulators in Scotland, Wales and Northern Ireland, and pharmacy regulation in Northern Ireland sits outside the GPhC.

Design biometrics around consent. Face matching needs explicit consent and a genuine non-biometric alternative, documented in a data protection impact assessment.

Keep the audit trail. Regulators expect records of how identity was checked, why a supply was made or refused, the delivery method and who received the medicine. Sensible re-verification points include changes to account details, delivery address or payment details, and supplies of medicines liable to misuse.

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 and checks, face match and biometric liveness, configurable by medicine risk.
- Video KYC sessions that can support consultations where regulators expect two-way communication or independent verification.
- Age verification and phone and email verification to support capacity, proxy and account security checks.
- No-code workflow builder with an audit trail of each check, supporting the records regulators expect to see on inspection.
- Cloud, on-premises or hybrid deployment to keep patient data in the UK or another jurisdiction with equivalent protection.

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

- **Health and Social Care Act 2008, section 10**, legislation.gov.uk, legislation.gov.uk/ukpga/2008/14/section/10
- **The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 (SI 2014/2936)**, Schedule 1, legislation.gov.uk/uksi/2014/2936
- **The Human Medicines Regulations 2012 (SI 2012/1916)**, regulations 214, 217 and 219, regulation 217, regulation 219
- **General Pharmaceutical Council, Guidance for registered pharmacies providing pharmacy services at a distance, including on the internet**, February 2025, sections 1, 3 and 4, assets.pharmacyregulation.org
- **General Pharmaceutical Council, Inspection outcomes and statutory enforcement powers**, pharmacyregulation.org
- **Care Quality Commission, How we monitor, inspect and regulate providers of online primary care**, cqc.org.uk
- **Care Quality Commission, announcement on action against online primary care providers** (2017), cqc.org.uk
- **NHS England, GP good practice guidance: Identity verification**, england.nhs.uk
- **Information Commissioner's Office (now the Information Commission), Biometric data guidance: How do we process biometric data lawfully?**, ico.org.uk
- **Information Commissioner's Office, Data (Use and Access) Act 2025**, ico.org.uk
- **Information Commissioner's Office, Monetary penalty: Advanced Computer Software Group Limited**, 26 March 2025, ico.org.uk
- **Data Protection Act 2018, section 157**, legislation.gov.uk/ukpga/2018/12/section/157
- **DSIT, Data Use and Access Act 2025: plans for commencement**, last updated 12 October 2026, gov.uk
- **Office for Digital Identities and Attributes, UK digital verification services trust framework (collection)**, last updated 11 June 2026, gov.uk
- **UK digital identity and attributes trust framework (0.4)**, last updated 9 June 2026, gov.uk