Identomat

COMPLIANCE GUIDE

Healthcare Compliance in the United States

COUNTRY United States | INDUSTRY Healthcare | LAST UPDATED 16 October 2026

KEY REGULATORS HHS Office for Civil Rights · Drug Enforcement Administration · Federal Trade Commission

Key takeaways

- There is no federal licence for telehealth, health apps or patient portals. Clinicians and pharmacies are licensed by each state, and anyone prescribing controlled drugs (for example opioids or stimulants) also needs a Drug Enforcement Administration (DEA) registration.
- Prescribing controlled drugs online to a patient who has never been seen in person is allowed only under temporary federal relief that ends on 31 December 2026. A permanent "special registration" for telemedicine has been proposed but is not yet law.
- Doctors who sign controlled-drug prescriptions electronically must have their own identity checked by an approved identity provider (or in person by their hospital) and must sign with two-factor authentication.
- Anti-money laundering rules do not apply to healthcare. Patient identity checks are driven by privacy law: providers must verify anyone asking for records whose identity they do not already know, online or in person, but no specific method is mandated.
- Health apps that are not working for a hospital, insurer or other regulated health provider fall outside the main health privacy law (HIPAA) but must still notify users of data breaches under a Federal Trade Commission (FTC) rule.

The United States market is open to digital health. Telehealth providers, online pharmacies, patient portals and consumer health apps all operate nationally, but under layered rules: state licensing of clinicians and pharmacies, federal controlled-substance law administered by the DEA, the HIPAA privacy and security rules enforced by the Department of Health and Human Services (HHS) Office for Civil Rights, and FTC rules for apps outside HIPAA.

The single biggest obstacle for a new entrant is the controlled-substance prescribing cliff. Business models that start patients on controlled medication by video alone rely on temporary relief that ends on 31 December 2026 unless it is extended again or replaced by a final rule.

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

Healthcare identity rules are split across federal agencies by subject, with licensing left to the states. There is no single digital health regulator.

Regulator	Remit relevant to identity	Level	Official site
HHS Office for Civil Rights (OCR)	HIPAA Privacy, Security and Breach Notification Rules: verification of requesters, access controls, enforcement	Federal	hhs.gov/ocr
Drug Enforcement Administration (DEA), Diversion Control	Controlled-substance registration, telemedicine prescribing, electronic prescribing of controlled substances, online pharmacies	Federal	deadiversion.usdoj.gov
Federal Trade Commission (FTC)	Health Breach Notification Rule for apps outside HIPAA; Red Flags Rule for creditors	Federal	ftc.gov
Assistant Secretary for Technology Policy / Office of the National Coordinator (ASTP/ ONC)	Health IT certification, information blocking, the Trusted Exchange Framework and Common Agreement (TEFCA)	Federal	healthit.gov

HHS Office of Inspector General (OIG)	Exclusion of individuals and entities from federal health programmes; civil money penalties	Federal	oig.hhs.gov
Centers for Medicare & Medicaid Services (CMS)	Telehealth payment rules and payer interoperability requirements	Federal	cms.gov
State medical and pharmacy boards	Licensing of clinicians and pharmacies, practice standards	State	Each state's own board

The National Institute of Standards and Technology (NIST) is a standard-setter, not a regulator: its digital identity guidelines bind health businesses only where a rule or contract adopts them.

2 Licensing and authorisation

Clinicians. Licensure to practise medicine, nursing or pharmacy is granted by each state, and a telehealth provider generally needs its clinicians licensed where the patient is located. This is a state-by-state patchwork with no federal licence that replaces it.

Controlled substances. A practitioner who prescribes controlled substances must hold a DEA registration authorising the relevant drug schedules. Under the Ryan Haight Online Pharmacy Consumer Protection Act of 2008, remote prescribing of controlled substances generally requires at least one in-person medical evaluation, subject to the statutory telemedicine exceptions (90 FR 61301).

Online pharmacies. A registered pharmacy that wants to dispense controlled substances over the internet must apply to DEA to modify its registration as an online pharmacy, and must comply with pharmacy licensing law in every state it ships from and to (21 CFR 1301.19).

Health apps and platforms. A technology platform that does not itself practise medicine needs no federal health licence. Its obligations follow from what it does: handling records for a provider makes it a HIPAA business associate, while a direct-to-consumer app that keeps a personal health record falls under the FTC rule. The proposed DEA special registration would, if finalised, also require certain direct-to-consumer telemedicine platforms to register.

3 Identity framework (AML rules do not apply)

Healthcare providers, telehealth platforms, pharmacies and health apps are not financial institutions under the Bank Secrecy Act regulations, whose list covers banks, broker-dealers, money services businesses, casinos and similar businesses (31 CFR 1010.100(t)). There is no customer identification programme, suspicious activity reporting or beneficial ownership obligation for a health business as such. A health business that also moves money for customers would need to assess that activity separately.

Identity obligations instead come from four sources:

HIPAA verification

Before any permitted disclosure, a covered entity must verify the identity and authority of a requester whose identity or authority it does not already know (45 CFR 164.514(h)).

HIPAA access control

The Security Rule requires procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed (45 CFR 164.312(d)).

Prescriber proofing

DEA rules require identity proofing and two-factor credentials for practitioners who sign controlled-substance prescriptions electronically (21 CFR 1311.105).

Identity theft programmes

A provider that is a "creditor" under the Fair Credit Reporting Act must run a written identity theft prevention programme under the Red Flags Rule (16 CFR Part 681).

Sanctions screening under the Office of Foreign Assets Control (OFAC) rules applies to every US person, including health businesses, but carries no healthcare-specific identity requirement.

4 Identity verification and onboarding

Patients

No federal rule prescribes the documents a patient must show to register with a provider or open a portal account. HIPAA requires verification where the requester's identity is not known but leaves the method to the covered entity, which may rely on documentation that reasonably appears valid on its face (45 CFR 164.514(h)(2)). For public officials the rule lists acceptable evidence: an agency badge in person, government letterhead in writing, or documentation that a person acts on an official's behalf. Patients exercising their right of

access must receive their records within 30 days, extendable once by up to 30 days with a written explanation (45 CFR 164.524), so verification must not become a barrier that delays access.

Prescribers of controlled substances

An individual practitioner must obtain a two-factor authentication credential from a credential service provider approved by the General Services Administration to proof identity at "Assurance Level 3" of NIST SP 800-63-1, or a digital certificate from a certification authority cross-certified with the Federal Bridge. The credential must be issued over two channels (21 CFR 1311.105). Alternatively, a hospital's credentialing office may proof its own practitioners in person by matching government photo identification to the person, checking state licence and DEA registration, and keeping a record of the proofing (21 CFR 1311.110).

The DEA rule has not changed since 2017 and still refers to SP 800-63-1. NIST has since replaced its four-level model with separate identity, authenticator and federation assurance levels, and the current revision is SP 800-63-4, which supersedes SP 800-63-3 (NIST SP 800-63-4). DEA has not published a mapping, so firms must document how their chosen proofing level meets the regulatory reference.

What the current NIST revision expects

Under SP 800-63A-4, Identity Assurance Level 2 (IAL2) may be delivered remotely and unattended, with or without biometrics, and requires validation of all core attributes including a government identifier. Remote biometric comparison requires presentation attack detection meeting an impostor attack presentation accept rate below 0.07, and documents must be captured live with document presence checks. IAL3 must be performed on site and attended by a proofing agent (NIST SP 800-63A-4).

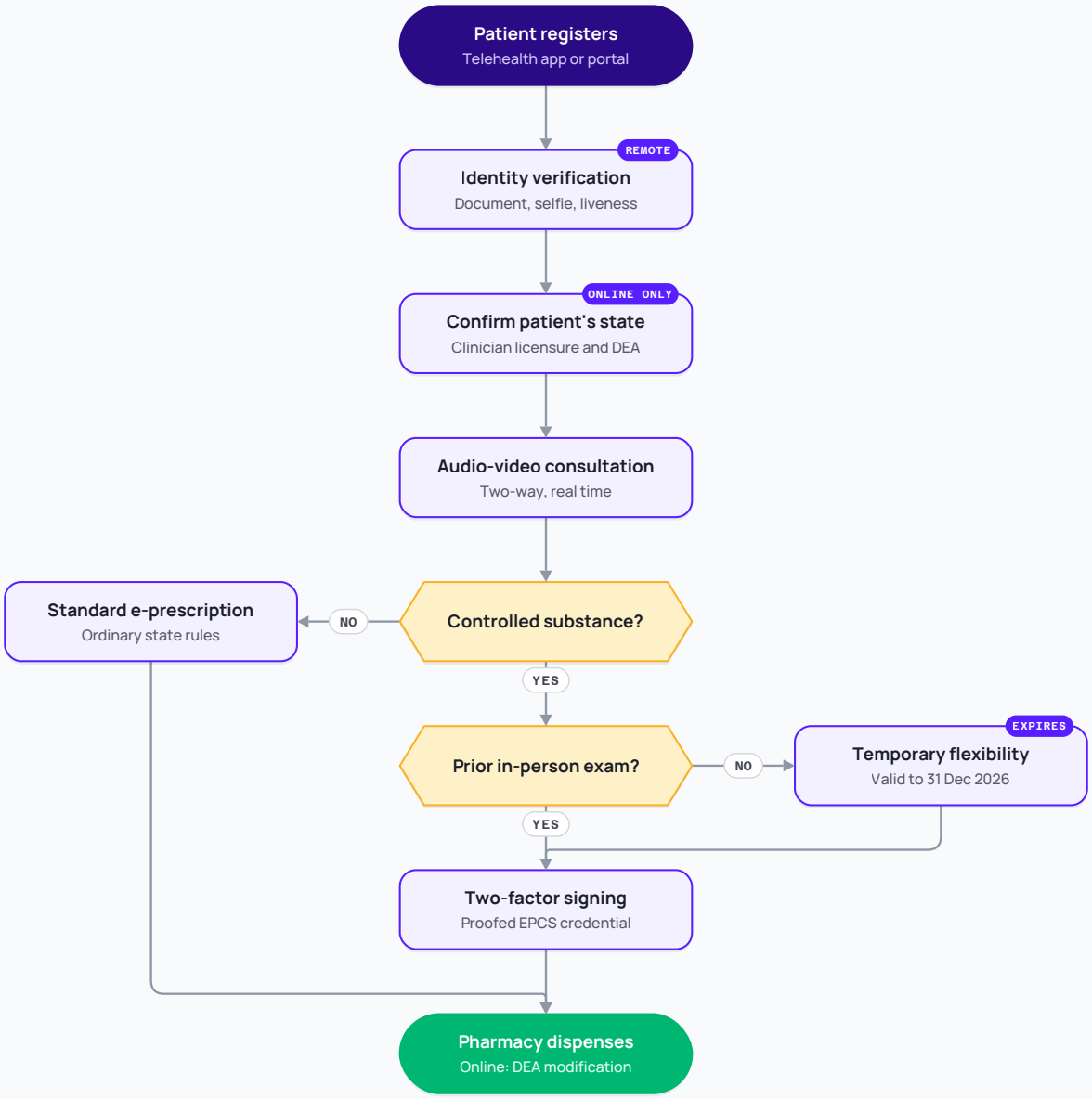


Figure 1. Telehealth onboarding and controlled-substance prescribing in the United States (as of October 2026).

5 Digital channels: what's different

Bottom line: patient identity rules are channel-neutral, but prescribing controlled substances to a new patient by video rests on temporary relief that ends on 31 December 2026.

Requirement	In person	Online / remote	Difference

Prescribing controlled substances to a new patient	In-person evaluation satisfies the Ryan Haight Act	Allowed without a visit only under temporary rule to 31 Dec 2026	`Differs`
Communication standard for telemedicine prescribing	Not applicable	Two-way, real-time audio-video; audio-only only in limited cases	`Differs`
Prescriber identity proofing for e-prescribing controlled drugs	Hospital may check photo ID in person	Approved credential service provider, credential issued over two channels	`Differs`
Verifying a patient who requests records	Required if identity not known; method not specified	Required if identity not known; method not specified	`Same`
Authenticating access to electronic records	Security Rule authentication applies	Security Rule authentication applies	`Same`
Dispensing controlled substances	Pharmacy registration and state licence	DEA online pharmacy modification and licences in each state served	`Differs`
Breach notification for health data	HIPAA Breach Notification Rule	HIPAA if a covered entity or business associate; FTC rule for other health apps	`Differs`

The telemedicine prescribing window

The fourth temporary rule, issued jointly by DEA and HHS, lets a DEA-registered practitioner prescribe Schedule II to V controlled substances by telemedicine without an in-person evaluation from 1 January to 31 December 2026, provided the prescription is for a legitimate medical purpose, is issued through an interactive telecommunications system as defined for Medicare, falls within the practitioner's registration, and meets the general prescription rules (90 FR 61301) `Temporary relief, ends 31 Dec 2026`. That system means real-time, two-way audio and video, with audio-only permitted for some services to patients at home (42 CFR 410.78(a)(3)). Separate final rules for buprenorphine treatment and Veterans Affairs patients took effect on 31 December 2025 and carry their own conditions.

Same rule, different evidence

HIPAA does not distinguish a request made through a portal from one made at a front desk. In practice the evidence differs: in person, staff can compare a photo ID with the person, while online the provider needs a documented remote method that is reasonable under the circumstances. Nothing in the Privacy Rule requires a NIST assurance level for patients.

Apps outside HIPAA

A consumer health app that keeps a personal health record and is not acting for a covered entity is subject to the FTC Health Breach Notification Rule rather than HIPAA (16 CFR 318.1).

Pending: the DEA special registration for telemedicine (`Proposed January 2025, not final`) would set permanent conditions, including registration of certain platforms.

6 Data protection and biometrics

There is no single federal data protection statute or authority in the United States. For health businesses, the relevant federal regimes are HIPAA for covered entities and their business associates, and FTC rules for others.

Identity data as health data. Identity documents, selfies and liveness results collected by a covered entity to register a patient become part of the protected health information it holds, and fall under the Security Rule's safeguards and the business associate rules if an identity vendor processes them on the provider's behalf. HIPAA policies and procedures documentation must be kept for six years from creation or last effective date (45 CFR 164.316).

Health apps. Vendors of personal health records and related entities must notify individuals, and in larger breaches the FTC and media, without unreasonable delay and no later than 60 calendar days after discovering a breach. Notice to the FTC for breaches of 500 or more people is due at the same time (16 CFR 318.4). The FTC amended the rule in 2024 (89 FR 47028), and an unauthorised disclosure, not only a hack, can be a breach (16 CFR 318.2).

Biometrics. No federal rule specific to healthcare governs biometric identifiers; several states have biometric privacy statutes that require notice or consent before collecting face geometry, and they apply alongside HIPAA.

Reproductive health records. HHS reports that a federal court vacated most of the 2024 HIPAA reproductive health privacy amendments on 18 June 2025 (HHS OCR) `Vacated by court`, although the text still appears in the codified regulation.

7 Sector-specific obligations

Electronic prescribing records

Records of electronic controlled-substance prescriptions must be kept electronically for two years, be readily retrievable and be available to DEA on request (21 CFR 1311.305). Institutions that proof their own practitioners must also keep a record of each proofing and credential issuance.

Health information exchange

TEFCA now has its own regulation, effective 15 January 2025, governing the qualified networks that exchange records nationally (89 FR 101772). Under Common Agreement Version 2.1, participants may offer Individual Access Services, letting patients retrieve their own records through an app, subject to express written consent and the framework's standard operating procedures (89 FR 93309).

Red Flags Rule: when a provider is a creditor

The Red Flags Rule applies to "creditors" as narrowed by Congress in 2010: businesses that regularly obtain or use consumer reports, report to credit bureaus, or advance funds repayable by the customer. A creditor that only advances funds for expenses incidental to its own service is excluded (15 U.S.C. 1681m(e)(4)). Billing a patient after treatment does not, on its own, bring a provider into scope; running credit checks or offering financing can.

Exclusion screening

Individuals and entities excluded by OIG cannot be paid by federal health programmes for items or services they furnish, and claims for such items or services expose the provider to civil money penalties (42 CFR 1003.200). Providers that bill federal programmes therefore screen staff, clinicians and vendors against the OIG exclusion list before engagement and on an ongoing basis.

8 Risk indicators and red flags

IDENTITY-ABUSE INDICATORS FOR HEALTH BUSINESSES

- **Altered documents**: identification that appears forged, or a photo that does not match the person (Red Flags Rule, Supplement A).
- **Inconsistent identifiers**: an address or Social Security number that does not match external sources, or an SSN listed as deceased.
- **Account change then request**: a change of contact details followed quickly by a request for records, refills or a new device.
- **Impersonated officials**: requests for records from "agencies" that lack letterhead, badge or documented authority (45 CFR 164.514(h)).
- **Phishing of staff**: credential theft leading to mass exposure of patient data, a recurring theme in recent OCR settlements.
- **Hacking of online systems**: unauthorised access to systems holding patient data, the subject of OCR's 2025 civil money penalty against Warby Parker.
- **Prescriber credential misuse**: e-prescriptions signed outside a practitioner's normal pattern or registration.

9 Enforcement and penalties

HIPAA. Civil money penalties are set per violation in four culpability tiers, with an annual cap for identical violations. After the January 2026 inflation adjustment (91 FR 3665), the figures in 45 CFR 102.3 are:

Tier (45 CFR 160.404(b)(2))	Per violation	Calendar-year cap
Did not know, and could not have known	$145 to $73,011	$2,190,294
Reasonable cause, not wilful neglect	$1,461 to $73,011	$2,190,294
Wilful neglect, corrected within 30 days	$14,602 to $73,011	$2,190,294
Wilful neglect, not corrected	$73,011 to $2,190,294	$2,190,294

Most cases end in resolution agreements with corrective action plans monitored for around three years. Recent examples include a $700,000 settlement with Ambry Genetics after a phishing attack exposed data of 225,000 patients (17 September 2026), a right of access settlement with Azul Vision (27 August 2026), and a $1,500,000 civil money penalty against Warby Parker in a hacking investigation (February 2025) (OCR resolution agreements).

FTC. Violations of the Health Breach Notification Rule are treated as violations of a trade regulation rule, with civil penalties of up to $53,088 per violation (16 CFR 318.7; 16 CFR 1.98).

DEA. Prescribing outside the telemedicine rules or the e-prescribing requirements can lead to revocation of registration; DEA publishes registrant decisions and orders in the Federal Register.

10 Recent changes and what to watch

- **31 December 2026**: telemedicine controlled-substance flexibilities expire unless extended or replaced `Temporary relief, ends 31 Dec 2026`. Plan for in-person evaluations or a permanent rule.
- **April 2026**: CMS proposed new payer interoperability and drug prior authorisation requirements; comments closed 15 June 2026 `Proposed`. Payer-facing apps should track the final rule.
- **February 2026**: HHS held a Tribal consultation on its pending proposal to modify the HIPAA Privacy Rule for care coordination and individual access `Proposed`.
- **18 June 2025**: most of the 2024 reproductive health privacy amendments vacated `Vacated by court`. Disclosure policies revert to the general Privacy Rule.
- **January 2025**: HIPAA Security Rule overhaul proposed; comments closed 7 March 2025 `Proposed, not final`. Security programmes should track it but cannot treat it as law.
- **January 2025**: DEA special registration for telemedicine proposed `Proposed, not final`. It would replace the temporary relief with permanent conditions.
- **15 January 2025**: TEFCA regulation took effect `In force`. Apps offering patients record access through the national network operate under its framework.

11 What this means for identity verification

Two identity populations. Health platforms verify patients under a flexible, reasonableness standard and verify prescribers under a fixed regulatory one. Design them separately: prescriber proofing must come from an approved credential service provider (or institutional in-person proofing) and end in a two-factor signing credential.

Document a standard for patients. Because HIPAA names no method, a documented remote method, such as document capture with face match and liveness aligned to IAL2 of SP 800-63A-4, gives a defensible basis for portal registration, record release and account recovery.

Location matters. Clinician and pharmacy licensing is state-based, so onboarding should capture and confirm where the patient is at the time of each consultation and each delivery.

Retention. Identity evidence held by a covered entity is protected health information; keep it no longer than needed, under business associate agreements with vendors, and keep e-prescribing records for two years.

Re-verification triggers. Changes of contact details, device or payment method followed by record or refill requests, and any requester whose identity is not known, should prompt step-up verification.

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 onboarding with ID document capture and verification, face match and biometric liveness, documented for HIPAA verification and account recovery.
- Identity checks for clinicians and staff, including ID document verification and ongoing screening against watchlists.
- Configurable no-code workflows that add step-up verification when contact details or devices change before record or refill requests.
- Cloud, on-premises or hybrid deployment to keep identity evidence within a covered entity's security programme.

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

- **Fourth Temporary Extension of COVID-19 Telemedicine Flexibilities for Prescription of Controlled Medications**, 90 FR 61301 (31 Dec 2025), federalregister.gov
- **21 CFR 1311.105, Requirements for obtaining an authentication credential, individual practitioners**, eCFR, ecfr.gov
- **21 CFR 1311.110, Authentication credentials for practitioners using an institutional practitioner's application**, eCFR, ecfr.gov
- **21 CFR 1311.305, Recordkeeping**, eCFR, ecfr.gov
- **21 CFR 1301.19, Special requirements for online pharmacies**, eCFR, ecfr.gov
- **42 CFR 410.78(a)(3), Interactive telecommunications system**, eCFR, ecfr.gov

- **45 CFR 164.514(h), Verification requirements**, eCFR, ecfr.gov
- **45 CFR 164.524, Access of individuals to protected health information**, eCFR, ecfr.gov
- **45 CFR 164.312, Technical safeguards**, eCFR, ecfr.gov
- **45 CFR 164.316, Policies and procedures and documentation requirements**, eCFR, ecfr.gov
- **45 CFR 102.3, Civil monetary penalty amounts**, as amended by 91 FR 3665 (28 Jan 2026), ecfr.gov; federalregister.gov
- **16 CFR Part 318, Health Breach Notification Rule** (318.1, 318.2, 318.4, 318.7), eCFR, ecfr.gov; amendments 89 FR 47028 (30 May 2024), federalregister.gov
- **16 CFR 1.98, Adjustment of civil monetary penalty amounts**, eCFR, ecfr.gov
- **16 CFR Part 681, Identity Theft Rules**, including Supplement A, eCFR, ecfr.gov
- **15 U.S.C. 1681m(e)(4), definition of creditor**, United States Code (2024 edition), govinfo.gov
- **42 CFR 1003.200, OIG civil money penalties**, eCFR, ecfr.gov
- **31 CFR 1010.100(t), Financial institution**, eCFR, ecfr.gov
- **NIST SP 800-63-4, Digital Identity Guidelines**, and **SP 800-63A-4, Identity Proofing and Enrollment**, pages.nist.gov; pages.nist.gov
- **Health Data, Technology, and Interoperability: TEFCA**, 89 FR 101772 (16 Dec 2024), federalregister.gov
- **Common Agreement for Nationwide Health Information Interoperability, Version 2.1**, 89 FR 93309 (26 Nov 2024), federalregister.gov
- **HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information** (proposed rule), 90 FR 898 (6 Jan 2025), federalregister.gov
- **Tribal Consultation on Proposed Modifications to the HIPAA Privacy Rule**, 91 FR 1481 (14 Jan 2026), federalregister.gov
- **CMS Interoperability Standards and Prior Authorization for Drugs** (proposed rule), 91 FR 19890 (14 Apr 2026), federalregister.gov
- **HIPAA and Reproductive Health**, HHS Office for Civil Rights, hhs.gov
- **HIPAA Resolution Agreements and Civil Money Penalties**, HHS Office for Civil Rights (reviewed 9 Oct 2026), hhs.gov