SmartSuite

Framework / Privacy / Global Privacy Regulations

HIPAA (45 CFR Parts 160 & 164) — 2013 Omnibus Rule

The HIPAA Omnibus Rule (78 FR 5566, 2013) made business associates directly liable, set the breach risk assessment and tiered penalties, and added GINA protections.



What it is

HIPAA, the Health Insurance Portability and Accountability Act of 1996, as amended by the 2013 Omnibus Rule, sets U.S. federal rules for the privacy, security, breach notification and enforcement of protected health information (PHI) in 45 CFR Parts 160 and 164. It binds covered entities (health plans, health care clearinghouses and health care providers) and, since the Omnibus Rule, business associates and their subcontractors directly. The HHS Office for Civil Rights (OCR) published the Omnibus Rule at 78 Fed. Reg. 5566 on January 25, 2013. It took effect on March 26, 2013, and organizations had to comply by September 23, 2013.

At a glance

PUBLISHER
U.S. Department of Health and Human Services (HHS), Office for Civil Rights

TYPE
Regulation

VERSION
HIPAA Omnibus Final Rule, 78 Fed. Reg. 5566 (45 CFR Parts 160 and 164)

EFFECTIVE
March 26, 2013 (compliance date September 23, 2013)

DOMAIN
Privacy

FAMILY
Global Privacy Regulations

REGION
United States

INDUSTRY
Healthcare & Life Sciences

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf

Why it matters

- **Business associates and subcontractors covered directly** The definition in 45 CFR 160.103 includes a subcontractor that creates, receives, maintains or transmits PHI for a business associate, and section 164.104(b) applies the standards to business associates where provided.
- **A breach is presumed** An impermissible use or disclosure is presumed to be a breach unless a risk assessment shows a low probability that the PHI has been compromised (section 164.402).
- **Stronger individual protections** Sale of PHI and marketing with remuneration need an authorization (section 164.508(a)(3) and (a)(4)), and a patient can restrict disclosures to a health plan for care paid in full out of pocket (section 164.522(a)(1)(vi)).
- **Genetic information protected** A health plan, except a long-term care issuer, may not use or disclose genetic information for underwriting (section 164.502(a)(5)(i)).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports HIPAA

Business Associate Register

Record each business associate and subcontractor with the contract status under sections 164.504(e) and 164.314(a), renewal dates and the owner of each agreement.

Risk Analysis and Safeguard Tracker

Record the risk analysis required by section 164.308(a)(1)(ii)(A), the risks found, the mitigation plan, owners and review dates.

Breach Risk Assessment Workflow

Run the four-factor assessment of section 164.402 for each incident, with the decision, the approver and the 60-day notification clock.

Breach Log and Notification Tracker

Keep the log of breaches under 500 people for the annual HHS report, and the media and HHS notice steps for larger breaches (sections 164.406 and 164.408).

Authorizations and Individual Requests

Track marketing and sale-of-PHI authorizations, fundraising opt-outs, electronic copy requests and out-of-pocket restriction requests (sections 164.508, 164.514, 164.522 and 164.524).

Notice of Privacy Practices Versions

Keep each version of the notice of privacy practices with its effective date, owner and approval, and record what changed (section 164.520).

Common framework mappings

CIS Controls v8.1 · COBIT 2019 · GLBA Safeguards Rule (16 CFR Part 314) · ISO 27001:2022 · ISO 27002:2022 · NIST CSF 2.0 · NIST 800-53 Rev.5 · PCI DSS 4.0.1 · SOC 2

Official resources

HIPAA Administrative Simplification Statute and Rules

Provides official text and explanation for HIPAA's administrative simplification provisions.

hhs.gov/hipaa/for-professionals/special-topics/hipaa-administrative-simplification-statute-and-rules/index.html

HIPAA Security Rule Guidance Material

Outlines detailed guidance on the HIPAA Security Rule standards and implementation specifications.

hhs.gov/hipaa/for-professionals/security/guidance/index.html

Summary of the HIPAA Privacy Rule

Provides an overview of the HIPAA Privacy Rule, outlining key provisions and requirements.

hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

HIPAA Omnibus Final Rule (78 Fed. Reg. 5566)

The Federal Register text of the January 25, 2013 final rule, with its preamble and amended regulation text.

govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf

Frequently asked questions

What did the HIPAA Omnibus Rule change?

It combined four rules published at 78 Fed. Reg. 5566. It made business associates and their subcontractors directly liable for parts of the Privacy and Security Rules, adopted the final Breach Notification Rule with an objective risk assessment, set tiered civil money penalties, and applied GINA to bar most health plans from using genetic information for underwriting. It also changed marketing, sale of PHI, fundraising, decedent and notice of privacy practices rules.

When did the Omnibus Rule take effect?

It took effect on March 26, 2013, and covered entities and business associates had to comply by September 23, 2013. An older business associate contract that met the earlier rules was deemed compliant until it was renewed or modified after that date, or until September 22, 2014, whichever came first (45 CFR 164.532(e)).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

When is an impermissible disclosure a reportable breach?

Under 45 CFR 164.402 it is presumed to be a breach unless the organization shows a low probability of compromise from a risk assessment of at least four factors: the nature and extent of the PHI, who used or received it, whether it was actually acquired or viewed, and how far the risk has been mitigated. Three narrow exceptions apply, such as an unintentional good-faith use by a workforce member.

What are the HIPAA civil money penalty tiers?

Section 160.404 has four tiers by culpability. As adjusted on January 28, 2026, per-violation amounts are $145 to $73,011 when the entity did not know, $1,461 to $73,011 for reasonable cause, $14,602 to $73,011 for willful neglect corrected within 30 days, and $73,011 to $2,190,294 for uncorrected willful neglect. Under a 2019 notice HHS applies a separate annual cap to each tier.

Has anything replaced the 2013 Omnibus Rule?

No. The 2024 reproductive health care privacy rule was vacated on June 18, 2025 in Purl v. HHS, except its changes to section 164.520 (apart from three vacated paragraphs). The January 6, 2025 proposal to revise the Security Rule (90 Fed. Reg. 898) has no final rule in the Federal Register as of October 14, 2026, so the 2013 rule text remains the base.

License included / downloadable: Yes The Omnibus Rule is a U.S. federal regulation published in the Federal Register and is in the public domain. The current regulation text is at 45 CFR Parts 160 and 164.

Full framework page and mappings: smartsuite.com/frameworks/hipaa-omnibus-rule-2013