

SAMPLE

AI Compliance Toolkit

The opening of AIC-Regulatory-Guide.docx, one of 6 files in the kit. <https://solasai.net/products/ai-compliance-toolkit/>

AI Regulatory Guide

HIPAA, the EU AI Act, the FTC Act and TCPA, legal ethics, and US state AI laws: what each requires of a small business that deploys AI, with the dates, the penalties, the enforcement record, and the sources

Product: AI Compliance Toolkit, version 3.0, 19 October 2026. **Classification:** Purchaser use only, customize before use. Solas AI, solasai.net.

How to use this document

Each chapter answers the same six questions for one regime: who it binds, what it requires of a business that uses AI rather than builds it, which dates matter, what the penalties are, what enforcement has looked like, and where the primary sources are. The dated rows in each "Key dates" table are copied into the Calendar sheet of the Self-Assessment Workbook. Every date, case, and citation in this guide was checked against a primary source (the regulation, the statute, the agency's own page, the court's opinion) on 19 October 2026; the sources are listed at the end of each chapter. Regulators move, so check the source before relying on a date more than a few months after that.

This guide is reference material, not legal advice. It tells you where the obligations are and what they say; it does not tell you what to do in your facts. Use it to brief counsel, not to replace them.

HIPAA and health information

Who it binds

HIPAA binds covered entities (health care providers that transmit health information electronically in connection with a standard transaction, health plans, and clearinghouses) and their business associates. A dental or medical practice that bills electronically is a covered entity. Any vendor that creates, receives, maintains, or transmits protected health information on the practice's behalf is a business associate (45 CFR 160.103), and the practice may let it do so only with satisfactory assurances documented in a written agreement that meets 45 CFR 164.504(e) (164.502(e)). An AI scheduling assistant, voice agent, note summariser, transcription service, or insurance verification tool that touches patient information is a business associate, and so is the model provider behind it when it sees the data.

There is no AI-specific HIPAA rule, and as of October 2026 the Department of Health and Human Services has proposed none. The only open HIPAA rulemaking is the Security Rule update described below. The existing Privacy, Security, and Breach Notification Rules apply to AI tools exactly as they apply to any other system that handles protected health information.

What it requires

The Privacy Rule governs use and disclosure. Uses for treatment, payment, and health care operations need no patient authorization, and AI tools performing those functions under a business associate agreement fit inside them. Marketing uses need written authorization (164.508(a)(3)). The minimum necessary standard (164.502(b)) applies to every disclosure to a business associate and to every prompt: a recall message needs a first name and an appointment type, not the chart. Where a task can be done on de-identified data, de-identification means either Expert Determination or Safe Harbor, which removes all eighteen listed identifiers including dates more specific than the year, most ZIP codes, device identifiers, and any other unique code (164.514(b)); free text is where identifiers survive. The Notice of Privacy Practices (164.520) is where patients learn, in general terms, how information is used and shared.

The Security Rule governs electronic protected health information. The risk analysis (164.308(a)(1)(ii)(A)) must cover every system that creates, receives, maintains, or transmits it, which now includes the AI tools and the places their transcripts, recordings, and logs are stored. Workforce training (164.308(a)(5)), access management (164.308(a)(3)), contingency planning (164.308(a)(7)), device and media controls (164.310(d)), and the technical safeguards of access control, audit controls, integrity, and transmission security (164.312) all extend to those systems. Required documentation (policies, risk analyses, agreements, training records) is retained for six years from its creation or the date it was last in effect (164.316(b)(2)). The business associate agreement must require the vendor to return or destroy protected health information at termination (164.504(e)(2)(ii)(J)).

The sample ends here. The full document runs about 10,930 words; the kit holds 6 files. Version 2.2, 19 October 2026. Buy it at <https://solasai.net/products/ai-compliance-toolkit/>, 14-day refund for any reason.