

PRIVACY

PHI and the model: what HIPAA requires when a language model touches the chart

ABSTRACT

A practice that sends chart text to a language model discloses protected health information to whoever operates the model. This review sets out what the HIPAA Privacy, Security and Breach Notification Rules require in that case, alongside 42 C.F.R. Part 2 and Tennessee's breach statute. A model vendor is a business associate, not a conduit, and must sign an agreement whose contents the rules prescribe. The rules set no retention period during the contract and say nothing about training, hosting location or ownership of output; those are contract terms. The re-identification and memorization evidence is weighed against the de-identification standard, and the pending Security Rule revision is given at its September 2026 status.

Type Regulatory review References 29 Reading time 15 min Last reviewed September 2026

1 HIPAA regulates the holder, not the model

A practice that sends part of a chart to a language model, to draft a note or a message reply, discloses protected health information to whoever operates the model. HIPAA does not regulate the model. It regulates covered entities and the persons who create, receive, maintain or transmit PHI on their behalf, chiefly through a written agreement whose minimum contents the regulations prescribe.^{1,2,3}

The short answer has four parts. A vendor that processes PHI to run a model is a business associate, and the conduit exception does not reach it. The rules require a business associate agreement and specify what it must say. They set no retention period while the contract runs, say nothing in § 164.504(e) about training a model, do not require domestic hosting and do not address who owns generated text; those are contract terms. And "HIPAA compliant" describes no regulatory status: HHS and its Office for Civil Rights (OCR) state that they do not certify any persons or products as HIPAA compliant.⁴

What follows reads the regulation text as codified in September 2026 and OCR guidance on it, with 42 C.F.R. Part 2 and Tennessee law. It is not legal advice.

18

identifiers the safe harbor method removes, including those of relatives, employers and household members

0.013%

of records re-identified in the only reviewed attack on health data de-identified to an existing standard

60 days

outer limit for a business associate to report a breach to the covered entity

2 A model vendor is a business associate, and not a conduit

The definition turns on verbs. A business associate is a person who, on behalf of a covered entity, “creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter”, and the term expressly includes a subcontractor that does the same on behalf of a business associate.¹ A model service receives the prompt, creates the output and maintains whatever it logs. A vendor that runs its model on another company’s cloud makes that company a subcontractor, from which it must obtain its own written agreement.^{1,2,3}

The conduit exception is narrow by design

The 2013 omnibus rule calls the conduit exception “a narrow one”, intended to exclude “only those entities providing mere courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet service providers (ISPs) providing mere data transmission services.”⁵ The line is between transient and persistent access. OCR’s October 2016 cloud computing guidance applies the same line: a cloud provider that lacks the decryption key for what it stores is still a business associate, and using one to maintain electronic PHI without an agreement violates the HIPAA Rules.⁶ A service that reads clinical text and writes new clinical text is not transmitting it.

Direct liability, and its limit

The omnibus rule took effect March 26, 2013, with compliance required by September 23, 2013, and made subcontractors directly subject to the rules as business associates are.⁵ OCR lists ten categories of business associate direct liability, among them Security Rule compliance, impermissible uses and disclosures, minimum necessary, breach notification and subcontractor agreements, and may act against business associates only for those.⁷ Obligations beyond the list reach the vendor through the agreement.

The duty to have an agreement is enforced on its own. In 2016 an orthopaedic clinic agreed to a \$750,000 settlement after releasing x-ray films and the PHI of approximately 17,300 patients, with no agreement in place, to a company that offered to transfer the images to electronic media in exchange for the silver in the film. OCR’s director called the requirement “more than a mere check-the-box paperwork exercise.”⁸ It was a settlement, not a judgment.

3 What the agreement must contain

A covered entity may disclose PHI to a business associate only on satisfactory assurance that it will be safeguarded, documented in a written contract meeting § 164.504(e), and the same structure runs from a business associate to each subcontractor.² The Security Rule repeats the requirement for electronic PHI.⁹ A business associate “may use or disclose protected health information only as permitted or required by its business associate contract” or as required by law.²

TABLE 1

Principal required contents of a business associate agreement under 45 C.F.R. § 164.504(e)(2) and § 164.314(a)(2)(i), paraphrased. The regulation text governs.

Provision	The agreement must	Citation
Permitted uses	State them, authorizing nothing the covered entity could not do itself, except the vendor's management and administration and data aggregation	§ 164.504(e)(2)(i) ³
No other use	Bar use or disclosure beyond the contract or the law	(e)(2)(ii)(A) ³
Safeguards	Require safeguards and Security Rule compliance for electronic PHI	(e)(2)(ii)(B); § 164.314(a)(2)(i)(A) ^{3,9}
Reporting	Require reports of uses not provided for, breaches of unsecured PHI and security incidents	(e)(2)(ii)(C); § 164.314(a)(2)(i)(C) ^{3,9}
Subcontractors	Bind them to the same restrictions and conditions	(e)(2)(ii)(D); § 164.314(a)(2)(i)(B) ^{3,9}
Individual rights	Support access, amendment and accounting of disclosures	(e)(2)(ii)(E)–(G) ³
Books and records	Open them to the Secretary	(e)(2)(ii)(I) ³
Termination	Require return or destruction if feasible, retaining no copies; otherwise extend protections and limit use	(e)(2)(ii)(J) ³
Right to terminate	Allow termination for violation of a material term	(e)(2)(iii) ³

The practice also carries a continuing duty. A covered entity that knew of a pattern of activity or practice by its business associate amounting to a material breach of the agreement is itself out of compliance, unless it took reasonable steps to cure the breach and, if those failed, terminated the arrangement where feasible.³

4 What the rules leave to contract

Training

Nothing in § 164.504(e) addresses using PHI to train a model; the permitted-uses clause decides it, and may authorize nothing the covered entity could not do itself, with two exceptions. Management and administration covers uses necessary for the vendor's own proper management and administration or its legal responsibilities.³ Data aggregation is the combining of PHI held for one covered entity with PHI held for another "to permit data analyses that relate to the health care operations of the respective covered entities."¹⁰ Whether training a model sold to other customers is such an analysis, the text does not say.

The wider door is de-identification. A covered entity may use a business associate to de-identify PHI "only to the extent such activity is authorized by their business associate agreement",¹¹ and information meeting the standard is not individually identifiable.² Unless the agreement also limits what the vendor may do with the result, a clause permitting de-identification leaves the rule with nothing to say about the vendor's later use of it, training included. A price concession given for data rights must also be read against the prohibition on selling PHI, which reaches disclosures for which the discloser "directly or indirectly receives remuneration" from the recipient, subject to listed exceptions.²

Retention, location and reporting

No retention period applies while the contract runs. At termination the vendor must return or destroy the PHI "if feasible"; if not, the agreement's protections extend to it and further use is limited to the purposes that make return or destruction infeasible.³ The duty covers information "created or received by the business associate on behalf of" the covered entity, so it reaches generated output; who owns that output is not a HIPAA question. Storing electronic PHI on servers outside the United States is permitted with an agreement, OCR says, though location-dependent risk belongs in the risk analysis.⁶ Breaches of unsecured PHI run on the breach rule's clock, set out in section 8; other security incidents and unauthorized uses must be reported, with no deadline in the text.^{3,9} The guidance does bar one commercial behavior: a cloud provider may not impermissibly use the data by blocking or terminating the customer's access to it.⁶

The label

HHS "does not endorse or otherwise recognize private organizations' 'certifications' regarding the Security Rule, and such certifications do not absolve covered entities of their legal obligations under the Security Rule."¹² OCR does not certify any persons or products as HIPAA compliant.⁴

TABLE 2

Terms that matter for a model vendor: what the regulation text fixes and what it leaves to the parties, as of September 2026.

Term	What the text fixes	Left open
Training on PHI	Only uses the agreement permits, within the § 164.504(e)(2)(i) ceiling ³	Whether training is permitted, and for whose benefit
De-identification by the vendor	Only if the agreement authorizes it; the result is outside the rule ¹¹	What the vendor does with de-identified data
Retention during the contract	No period stated ³	Prompt, output and log retention
End of the contract	Return or destroy if feasible; otherwise extend protections ³	What counts as infeasible
Hosting location	Permitted abroad; risk to be analyzed ⁶	Region commitments
Incident reporting	Breaches on the breach rule's clock; other incidents reported ^{3,9}	Deadlines for incidents that are not breaches
Generated output	PHI when identifiable; within return or destruction ³	Ownership and reuse
"HIPAA compliant"	No federal certification exists ^{4,12}	Nothing; the label has no regulatory meaning

WHAT THIS SECTION DOES NOT CLAIM

It reads regulation text and OCR guidance. It does not assess any vendor's agreement or whether a particular clause is adequate, and it is not legal advice. Several questions it identifies, including whether model training can qualify as data aggregation, have no answer in the text, and this review located no agency guidance that answers them.

5 Minimum necessary applies to the prompt

The minimum necessary standard binds both parties: "a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."² Its exceptions begin with disclosures to or requests by a health care provider for treatment, and none is written for a vendor that is not itself a treating provider.

For a language model this is a question about how context is assembled. A design that sends the whole chart where a medication list would serve has a minimum necessary question to answer. The Security Rule adds a second reason to know what leaves the system: its risk analysis must be “an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.”⁹ A flow to a model vendor, and into its logs, belongs in that assessment. Neither provision prescribes an architecture; both require knowing what was sent, and why.

6 De-identification: the standard, and what re-identification studies measured

Health information is not individually identifiable when it does not identify an individual and there is “no reasonable basis to believe that the information can be used to identify an individual.”¹³ Two methods satisfy the standard. Under expert determination, a qualified person applying statistical and scientific principles determines and documents that the risk is very small that the information could be used, alone or with other reasonably available information, by an anticipated recipient to identify an individual.¹³ OCR’s guidance adds that no explicit numerical level of risk universally meets that threshold.¹¹

Under safe harbor, 18 listed identifiers “of the individual or of relatives, employers, or household members of the individual” are removed, among them geographic units smaller than a state except a three-digit ZIP area of more than 20,000 people, all date elements except year, and ages over 89; and the covered entity must have no actual knowledge that what remains could identify the individual.¹³ The guidance says the standard makes no distinction between structured fields and free text: a listed identifier must be removed wherever it appears. Its example of actual knowledge is a record listing a patient’s occupation as former president of the State University.¹¹ Clinical narrative, the material a language model consumes, is where both conditions are hardest to meet.

The famous figures, and what they are figures of

Sweeney’s 2000 working paper estimated from 1990 census data that 87% of the US population, 216 million of 248 million, was likely unique on 5-digit ZIP code, gender and date of birth.¹⁴ Golle, re-analyzing in 2006, obtained 61% for 1990 and 63% for 2000 on the same attributes, and speculated that the difference may arise partly because the 1990 census did not tabulate data directly by ZIP code.¹⁵ Either figure concerns a combination that safe harbor breaks: it reduces the ZIP code to at most three digits and the date of birth to its year, leaving only gender intact.¹³ They explain why the method is written as it is; they are not evidence that data meeting it can be re-identified.

Rocher and colleagues modelled the problem. Their generative copula-based method predicted individual uniqueness across 210 populations with AUC scores of 0.84 to 0.97, and their abstract states that 99.98% of Americans would be correctly re-identified in any dataset using 15 demographic attributes.¹⁶ In the body the same figure is stated as 15 demographic attributes rendering 99.98% of

people in Massachusetts unique, with uniqueness estimated on that state's population from the census 5% Public Use Microdata Sample. It is a modelled estimate, framed by the authors against the GDPR standard, not a measured re-identification of data de-identified under either HIPAA method.

The systematic review of actual attacks points the other way. El Emam and colleagues found 14 eligible attacks; on average about a quarter of records were re-identified (0.26, 95% CI 0.046 to 0.478), and 0.34 in attacks on health data (95% CI 0 to 0.744).¹⁷ Only 2 of the 14 used data de-identified to an existing standard, and the single one on health data re-identified 0.013% of records. The authors judged the evidence, dominated by small studies on data not de-identified to existing standards, insufficient to draw conclusions about de-identification's efficacy. It does not show that de-identification works; it shows that the well-known failures mostly involved data that had not met a standard.

Free text is where the standard is hardest to meet. In the 2014 i2b2/UTHealth shared task on de-identifying longitudinal clinical narratives, three of 10 teams' systems achieved F1 scores above .90.¹⁸ The task predates current models and scored a broader set of entities than the HIPAA identifiers, and an F1 score mixes missed identifiers with false alarms, so the headline figure gives no residual-identifier rate; its point is that automated de-identification of narrative is measured as an error rate, while safe harbor requires every listed identifier removed.

7 Training is the term that decides what the weights contain

Whether a vendor trains on customer data matters because models retain some of what they are trained on. Carlini and colleagues extracted hundreds of verbatim sequences from GPT-2's training data, including public personally identifiable information such as names, phone numbers and email addresses, even though each of those examples appeared in just one document in the training data; larger models were more vulnerable.¹⁹ Nasr and colleagues built attacks that undo a model's alignment and recovered thousands of training examples from proprietary aligned production models, including ChatGPT.²⁰

The clinical evidence is thinner, and so far less alarming. Lehman and colleagues tried to recover patient names and their associated conditions from BERT trained on the MIMIC-III corpus, found that simple probing methods could not meaningfully extract sensitive information, and cautioned that more sophisticated attacks may succeed.²¹ BERT is not a generative model; the authors adapted the GPT-2 extraction approach to it, and the study predates the attacks on aligned models.^{19,20,21}

The regulatory consequence runs through the termination clause. PHI in a prompt log can be deleted; PHI that has shaped a model's parameters cannot be returned, and the rule does not say whether it can be destroyed short of discarding the model. Its fallback where return or destruction is infeasible is to extend the agreement's protections and limit further use to the purposes that make it infeasible.³ This review located no regulation or OCR guidance on whether trained parameters maintain the PHI they were trained on. A contract that excludes training avoids the question; one that permits training accepts it.

WHAT THE MEMORIZATION STUDIES DO NOT ESTABLISH

The extraction results concern general-purpose models, and the personal information recovered from GPT-2 was public web text; the one clinical study found little leakage from a non-generative model. No study reviewed here measures how much PHI can be extracted from a generative model trained on clinical records, so the risk is established in kind, not in rate. Use without training raises a simpler question: prompts and outputs still pass through the vendor and persist in whatever it logs.

8 Breach, substance use records and the Tennessee statute

An acquisition, access, use or disclosure of PHI that the Privacy Rule does not permit is presumed to be a breach unless the covered entity or business associate demonstrates a low probability of compromise, based on at least four factors: the nature and extent of the PHI, including identifiers and likelihood of re-identification; the unauthorized person who used or received it; whether it was actually acquired or viewed; and the extent of mitigation.²² A note pasted into a consumer chatbot with no agreement in place is, on the text, presumed a breach until that assessment shows otherwise.

A business associate must notify the covered entity without unreasonable delay and no later than 60 calendar days after discovery, counting from the first day the breach is known, or with reasonable diligence would have been known, to any of its employees, officers or other agents other than the one committing it.²² The covered entity has the same outer limit for notifying individuals; breaches of 500 or more individuals go to HHS contemporaneously, and smaller ones are logged and reported within 60 days after the end of the calendar year.²²

42 C.F.R. Part 2

For a pain practice, Part 2 sits beside HIPAA. Its 2024 final rule, 89 Fed. Reg. 12472–12631 (Feb. 16, 2024), implements section 3221 of the CARES Act; it took effect April 16, 2024, with compliance required by February 16, 2026.²³ It permits a single patient consent for all future uses and disclosures for treatment, payment and health care operations; lets a covered entity or business associate that receives records under that consent redisclose them as HIPAA allows; applies HITECH breach notification to breaches of records by Part 2 programs; and extends the limits on using the records in proceedings against the patient to administrative and legislative proceedings.²³ OCR announced that it would begin accepting Part 2 complaints and breach notifications on February 16, 2026.²⁴

Whether a practice is itself a program turns on definitions. A program includes a person, other than a general medical facility, that “holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment”, and it is federally assisted if, among other routes, it participates in Medicare or is registered under the Controlled Substances Act “to the extent the controlled substance is used in the treatment of substance use disorders.”²⁵ A treating provider not subject to Part 2 may record a patient’s substance use disorder and its treatment without thereby making its own record a Part 2 record; records received from a program carry the terms of the consent under which they arrived. Where a program uses a model vendor, the vendor’s place in the rule is as a qualified service organization, a status that requires a written agreement with the program and that includes a person meeting the HIPAA business associate definition for a program that is also a covered entity.²⁵ One chart can therefore hold the practice’s own documentation and program records under different rules, so a model pipeline needs the source and consent of each document to travel with it as data.

Tennessee

Tennessee’s breach statute adds less than its citation suggests. Tenn. Code Ann. § 47-18-2107 requires notice within 45 days of discovery or notification of a breach, but defines personal information as a name combined with a Social Security number, driver license number, or account, credit or debit card number with any required code or password, a list with no health information in it. Subsection (i) provides that the section does not apply to any information holder that is subject to the Health Insurance Portability and Accountability Act of 1996.²⁶ For a HIPAA-covered practice, on the face of the statute, the federal breach rule is the operative one.

9 What is pending, and what survives

The pending change that would alter these obligations is the Security Rule proposal, *HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information*, 90 Fed. Reg. 898–1022 (Jan. 6, 2025), RIN 0945-AA22, whose comment period closed March 7, 2025.²⁷ As HHS summarized it, the proposal would make all implementation specifications required, with limited exceptions; require encryption of electronic PHI at rest and in transit, and multi-factor authentication, each with limited exceptions; require a technology asset inventory and network map revised at least once every 12 months; require business associates to verify to covered entities at least once every 12 months, through a subject matter expert’s written analysis and a written certification, that required technical safeguards are deployed; and require business associates to notify covered entities no later than 24 hours after activating a contingency plan.²⁸ It also carried a request for information on new and emerging technologies, artificial intelligence among them.²⁷

None of it is law. As of September 2026 the proposal is the only document published in the Federal Register under its RIN, and the latest Unified Agenda lists it among long-term actions, with final action projected for July 2027.^{27,29}

HIPAA settles two questions about a model vendor. It decides whether PHI may reach the vendor at all, which is only under a written agreement with prescribed contents, and it binds the vendor directly on security, impermissible use, minimum necessary and breach notice.^{3,7} It does not decide how long prompts and outputs persist, where they are processed, whether they train a model and for whose benefit, or who owns what the model writes. A commitment on any of those exists only if the contract states it.

Three developments would narrow what is open: OCR guidance on whether cross-customer model training can be data aggregation, a statement on whether trained parameters maintain PHI for the purposes of return and destruction, and a final Security Rule. Until then the unit of compliance is the agreement, and the terms that matter most for a model are the ones HIPAA does not supply.

REFERENCES

Entries 1 to 7, 9 to 13, 22, 23, 25 and 26 are regulations, statutes and agency guidance: cite them for what they require, not as evidence of risk. Entry 27 is a proposed rule that is not in force, entries 28 and 29 are the agency's summary of it and the government's scheduling projection, and entries 8 and 24 are enforcement announcements rather than rulings. The empirical argument rests on entries 16 to 21, of which 17 is the only systematic review; entry 14 is an unreviewed working paper cited for the figure it originated, entry 15 is a four-page workshop paper, and entry 26 was read from an unofficial reproduction of the Tennessee Code because the official sources could not be retrieved.

1. U.S. Department of Health and Human Services. *Definitions: business associate; subcontractor; protected health information*. 45 C.F.R. § 160.103 (current as of Sept. 2026). [ecfr.gov](https://www.ecfr.gov)

REGULATION

2. U.S. Department of Health and Human Services. *Uses and disclosures of protected health information: General rules*. 45 C.F.R. § 164.502, including (a)(3), (a)(5)(ii), (b), (d) and (e).

[ecfr.gov](https://www.ecfr.gov)

REGULATION

3. U.S. Department of Health and Human Services. *Uses and disclosures: Organizational requirements*. 45 C.F.R. § 164.504(e), business associate contracts. [ecfr.gov](https://www.ecfr.gov)

REGULATION

4. Office for Civil Rights, U.S. Department of Health and Human Services. *What You Should Know About OCR HIPAA Privacy Rule Guidance Materials* (Be Aware of Misleading Marketing Claims). Content last reviewed July 26, 2013. [hhs.gov](https://www.hhs.gov)

GUIDANCE

5. Office for Civil Rights, U.S. Department of Health and Human Services. *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules*. Final rule. 78 Fed. Reg. 5566–5702 (Jan. 25, 2013); Doc. No. 2013-01073; effective Mar. 26, 2013; compliance Sept. 23, 2013. [federalregister.gov](https://www.federalregister.gov) REGULATION

6. Office for Civil Rights, U.S. Department of Health and Human Services. *Guidance on HIPAA & Cloud Computing*. Published Oct. 2016; content last reviewed Dec. 23, 2022. [hhs.gov](https://www.hhs.gov) GUIDANCE

7. Office for Civil Rights, U.S. Department of Health and Human Services. *Direct Liability of Business Associates*. Fact sheet; content last reviewed July 16, 2021. [hhs.gov](https://www.hhs.gov) GUIDANCE

8. Office for Civil Rights, U.S. Department of Health and Human Services. *\$750,000 settlement highlights the need for HIPAA business associate agreements* (Raleigh Orthopaedic Clinic, P.A.). Announced Apr. 19, 2016. [hhs.gov](https://www.hhs.gov) GOVERNMENT REPORT

9. U.S. Department of Health and Human Services. *Security standards: Administrative safeguards; Organizational requirements*. 45 C.F.R. §§ 164.308(a)(1)(ii)(A)–(B), 164.308(b), 164.314(a). [ecfr.gov](https://www.ecfr.gov) REGULATION

10. U.S. Department of Health and Human Services. *Definitions: data aggregation; health care operations*. 45 C.F.R. § 164.501. [ecfr.gov](https://www.ecfr.gov) REGULATION

11. Office for Civil Rights, U.S. Department of Health and Human Services. *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*. 2012. [hhs.gov](https://www.hhs.gov) GUIDANCE

12. Office for Civil Rights, U.S. Department of Health and Human Services. *Are we required to “certify” our organization’s compliance with the standards of the Security Rule?* FAQ; content last reviewed July 26, 2013. [hhs.gov](https://www.hhs.gov) GUIDANCE

13. U.S. Department of Health and Human Services. *Other requirements relating to uses and disclosures of protected health information*. 45 C.F.R. § 164.514(a)–(c), de-identification. [ecfr.gov](https://www.ecfr.gov) REGULATION

14. Sweeney L. *Simple Demographics Often Identify People Uniquely*. Carnegie Mellon University, Data Privacy Working Paper 3. 2000. dataprivacylab.org PREPRINT

15. Golle P. *Revisiting the Uniqueness of Simple Demographics in the US Population*. Proceedings of the 5th ACM Workshop on Privacy in Electronic Society (WPES '06). 2006:77–80. [doi:10.1145/1179601.1179615](https://doi.org/10.1145/1179601.1179615) CROSS-SECTIONAL

16. Rocher L, Hendrickx JM, de Montjoye Y-A. *Estimating the success of re-identifications in incomplete datasets using generative models*. Nature Communications. 2019;10(1):3069. doi:10.1038/s41467-019-10933-3 CROSS-SECTIONAL
17. El Emam K, Jonker E, Arbuckle L, et al. *A Systematic Review of Re-Identification Attacks on Health Data*. PLoS ONE. 2011;6(12):e28071. doi:10.1371/journal.pone.0028071 SYSTEMATIC REVIEW
18. Stubbs A, Kotfila C, Uzuner Ö. *Automated systems for the de-identification of longitudinal clinical narratives: Overview of 2014 i2b2/UTHealth shared task Track 1*. Journal of Biomedical Informatics. 2015;58(Suppl):S11–S19. doi:10.1016/j.jbi.2015.06.007 BENCHMARK
19. Carlini N, Tramèr F, Wallace E, et al. *Extracting Training Data from Large Language Models*. Proceedings of the 30th USENIX Security Symposium (USENIX Security 21). 2021:2633–2650. [usenix.org](https://www.usenix.org) BENCHMARK
20. Nasr M, Rando J, Carlini N, et al. *Scalable Extraction of Training Data from Aligned, Production Language Models*. International Conference on Learning Representations (ICLR 2025). 2025. proceedings.iclr.cc BENCHMARK
21. Lehman E, Jain S, Pichotta K, et al. *Does BERT Pretrained on Clinical Notes Reveal Sensitive Data?* Proceedings of the 2021 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies. 2021:946–959. doi:10.18653/v1/2021.naacl-main.73 BENCHMARK
22. U.S. Department of Health and Human Services. *Notification in the Case of Breach of Unsecured Protected Health Information*. 45 C.F.R. Part 164, Subpart D, §§ 164.402, 164.404, 164.408, 164.410. ecfr.gov REGULATION
23. Office for Civil Rights and Substance Abuse and Mental Health Services Administration, U.S. Department of Health and Human Services. *Confidentiality of Substance Use Disorder (SUD) Patient Records*. Final rule. 89 Fed. Reg. 12472–12631 (Feb. 16, 2024); Doc. No. 2024-02544; RIN 0945-AA16; effective Apr. 16, 2024; compliance Feb. 16, 2026. federalregister.gov REGULATION
24. U.S. Department of Health and Human Services. *Office for Civil Rights Announces Civil Enforcement Program for Confidentiality of Substance Use Disorder Patient Records*. Press release, Feb. 13, 2026. hhs.gov GOVERNMENT REPORT
25. U.S. Department of Health and Human Services. *Confidentiality of Substance Use Disorder Patient Records: Definitions; Applicability*. 42 C.F.R. §§ 2.11, 2.12 (current as of Sept. 2026). ecfr.gov REGULATION
26. Tennessee General Assembly. *Release of personal consumer information*. Tenn. Code Ann. § 47-18-2107 (2025), as amended by 2016 Tenn. Pub. Acts ch. 692 and 2017 Tenn. Pub. Acts ch. 91; read from an unofficial reproduction. law.justia.com STATUTE

- 27.** Office for Civil Rights, U.S. Department of Health and Human Services. *HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information*. Proposed rule. 90 Fed. Reg. 898–1022 (Jan. 6, 2025); Doc. No. 2024-30983; RIN 0945-AA22; comments closed Mar. 7, 2025. [federalregister.gov](https://www.federalregister.gov) **PROPOSED RULE**
- 28.** Office for Civil Rights, U.S. Department of Health and Human Services. *HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information*. Fact sheet, Dec. 27, 2024. [hhs.gov](https://www.hhs.gov) **GOVERNMENT REPORT**
- 29.** Office of Information and Regulatory Affairs. *2026 Unified Agenda of Federal Regulatory and Deregulatory Actions: HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information, RIN 0945-AA22*. Long-term actions; final action projected July 2027. [reginfo.gov](https://www.reginfo.gov) **GOVERNMENT REPORT**

RELATED PAPERS

Regulating AI in certified EHR technology

The certification and device regimes that reach the same feature from other directions

Retrieval over the chart

How context is assembled, which is where the minimum necessary question is decided

Ransomware and the independent practice

The Security Rule and breach duties when the incident is an attack