

SECURITY

Ransomware and the independent practice: what the breach record shows

ABSTRACT

Ransomware is usually framed as a threat to a practice's own network. This review reads the federal breach record, the peer-reviewed studies of attacks on care delivery and the rule text as of September 2026. Hacking accounted for 81% of large breach reports in 2024 and business associates for 85% of affected individuals; the Change Healthcare attack alone affected about 192.7 million people and disrupted practice cash flow for weeks. Hospital studies show falling volume and higher in-hospital mortality during attacks. The commonly recommended controls rest mostly on guidance and case evidence, the one randomized trial located, of phishing training, found little effect, and the 2025 Security Rule proposal is not final.

Type Evidence review References 29 Reading time 14 min Last reviewed September 2026

1 Most of a practice's exposure sits in someone else's system

Ransomware is usually presented to a small practice as a problem of its own network: a clicked link, an unpatched server, a locked front-desk screen. This paper asks what the record shows instead: how often hacking and ransomware are reported, whose systems held the records, what attacks have done to care and revenue, and which controls have evidence rather than endorsement. The sources are federal breach reports to Congress, peer-reviewed studies of attacks on care delivery, testimony and filings on the largest attack, and the rule text as it stands in September 2026.

The short answer has three parts. In the most recent year of federal data, hacking accounted for 81% of large breach reports and 99% of affected individuals, and breaches reported by business associates made up 16% of reports but 85% of the people affected.¹ For an independent practice, the largest recent exposure arrived through a clearinghouse, not through its own front door. The measured harms are real and mostly operational: hospital volume falls, in-hospital mortality rises among patients already admitted, neighboring emergency departments absorb the load, and practices lose cash flow when a vendor goes dark. The controls with the broadest support are unglamorous, and the support is mostly guidance, case evidence and vendor analysis; the one randomized trial found here tested staff awareness training and found it did little.

2 The federal record counts breached records, not ransomware

HIPAA’s breach notification rule produces the federal census. A covered entity notifies affected individuals without unreasonable delay and no later than 60 calendar days after discovery; breaches affecting 500 or more people go to the Secretary at the same time, while smaller ones are logged and reported within 60 days after the end of the calendar year.² The Office for Civil Rights (OCR) summarizes both streams in an annual report to Congress.

The two most recent reports describe a record dominated by hacking (Table 1). OCR received 732 reports of large breaches for 2023, affecting approximately 113,173,613 individuals, and 663 for 2024, affecting approximately 242,908,056.^{1,3} Reports fell and individuals more than doubled, because one 2024 breach, a ransomware attack on the servers of a health care clearinghouse, affected approximately 192,000,000 people on its own.¹ Small breaches are numerous and individually minor: 74,299 reports for 2024, affecting approximately 340,618 people in total.¹

TABLE 1
Breaches of unsecured protected health information reported to OCR that occurred in calendar years 2023 and 2024.

Measure	2023 ³	2024 ¹
Reports affecting 500 or more	732	663
Individuals affected	~113,173,613	~242,908,056
Hacking/IT incidents: reports	590 (81%)	534 (81%)
Hacking/IT incidents: individuals	108,725,761 (96%)	241,582,022 (99%)
Reported by business associates: reports	152 (21%)	106 (16%)
Reported by business associates: individuals	55,519,648 (49%)	206,921,071 (85%)
Largest single breach	~11,270,000; malware, provider servers	~192,000,000; ransomware, clearinghouse servers
Reports affecting fewer than 500	68,315	74,299

OCR’s breach categories do not separate ransomware. Jiang, Ross and Bai identified it within the hacking category from the free-text descriptions of 6,468 unique large breaches reported from October 2009 to October 2024, looking for ransom demands, cryptocurrency payment, encryption of systems or named ransomware groups.⁴ Hacking rose from 4% of breaches in 2010 (8 of 216) to 81% in 2024 (457 of 566). Ransomware’s share of breach reports peaked at 31% in 2021 (222 of 715) and fell to 11% in 2024 (61 of 566), a year the authors note is incomplete because their sample ended on 31 October. By people rather

than reports the picture inverts: ransomware has affected more than half of all patients whose records were breached every year since 2020, and 69% in 2024. Across 2010 to 2024 it accounted for 39% of 732 million affected records.

The denominator decides the headline. “Ransomware causes most health care breaches” is not what these data show by count of incidents; it is what they show by count of people, and in 2024 that count is dominated by a single event. The authors recommend a mandatory ransomware field in OCR reporting, which would make the question answerable without text-mining.⁴

3 Clinics are attacked most often; in 2024 a clearinghouse exposed the most people

Practices are not bystanders. Neprash and colleagues built a database of 374 ransomware attacks on US health care delivery organizations from 2016 through 2021, which exposed the protected health information of nearly 42 million patients.⁵ Clinics of all specialties were the most common type of organization attacked, in 216 attacks (57.8%), against 82 (21.9%) involving hospitals; the categories were non-exclusive.

The volume of exposure runs the other way. In 2024 the 106 large breaches reported by business associates, the vendors that handle protected information on a covered entity’s behalf, accounted for 85% of all affected individuals.¹ The 2023 figure was 49%.³

85%

of individuals in 2024 large breaches, from business-associate reports

~192.7M

individuals affected by the Change Healthcare attack

+34–38%

relative rise in in-hospital mortality among patients already admitted when an attack began

The Change Healthcare attack is the case most relevant to an independent practice. In written testimony to the Senate Finance Committee, UnitedHealth Group’s chief executive stated that on 12 February 2024 criminals used compromised credentials to reach a Change Healthcare Citrix remote-access portal, that “the portal did not have multi-factor authentication”, and that ransomware was deployed nine days later, after the attackers had moved laterally and exfiltrated data.⁶ Change filed its breach report with OCR on 19 July 2024.⁷

The size of the breach is sometimes quoted from an earlier stage. The figure of 100 million, which a 2025 research letter still used,⁴ matches the number of individual notices Change had told OCR it had sent by 22 October 2024; it was not a final count of people affected. On 24 January 2025 Change reported approximately 190 million individuals affected, and on 31 July 2025 approximately 192.7 million.⁷ For

cost, the primary source is the company's own accounting: UnitedHealth's full-year 2024 results attribute \$3,090 million to the attack before tax, comprising \$2,223 million in direct response costs and \$867 million in revenue lost to business disruption.⁸ These are the company's own figures.

The lesson for a practice is structural. Its own multifactor authentication protects its own accounts, not a vendor's remote-access portal. Its patients were exposed, and its claims stopped, through a system it neither ran nor could inspect.

4 When the clearinghouse stops, the practice's cash stops

The best-documented practice-level effect of the Change attack is financial, and it comes from surveys rather than claims data. The American Medical Association ran an informal survey through state and specialty medical societies from 26 March to 3 April 2024.⁹ Of more than 1,400 respondents, 1,097 were in practices of 10 or fewer physicians and 432 in single-provider practices. Eighty percent reported lost revenue from unpaid claims and 78% from claims they could not submit; 55% had used personal funds to cover practice expenses, 44% could not buy supplies and 31% could not make payroll. Forty-eight percent had engaged an alternative clearinghouse. A follow-up survey from 19 to 24 April, with more than 590 respondents and a respondent pool that differed from the first, found 62% using personal funds, 34% unable to make payroll and 29% relying on private bank loans.

Federal and company relief shows the scale of the liquidity gap without measuring it. The Centers for Medicare & Medicaid Services issued accelerated payments totaling more than \$2.55 billion to over 4,200 Part A providers and 4,722 advance payments totaling more than \$717.18 million to Part B suppliers, and stopped accepting applications after 12 July 2024.¹⁰ UnitedHealth's chief executive testified that the company had advanced more than \$6.5 billion in accelerated payments and no-interest, no-fee loans to thousands of providers.⁶ Both were advances and loans, not grants.

WHAT THE PRACTICE SURVEYS DO NOT ESTABLISH

The AMA surveys are self-selected samples distributed through professional societies and describe respondents, not practices nationally; the two waves did not follow the same respondents. They show that a vendor outage can starve a small practice of cash within weeks. They do not measure how many practices were affected, how much revenue was lost, or how long recovery took. No peer-reviewed estimate of practice-level revenue loss from the Change attack was read for this review.

5 Attacks measurably harm care, and the evidence comes from hospitals

Of the 374 attacks in the Neprash database, 166 (44.4%) disrupted care delivery: electronic system downtime in 156 (41.7%), cancelled scheduled care in 38 (10.2%) and ambulance diversion in 16 (4.3%).⁵ Annual attacks more than doubled from 43 in 2016 to 91 in 2021. Over the period, attacks increasingly hit large multi-facility organizations, exposed more records, exceeded mandatory reporting windows more often and became less likely to end in recovery from backup. Only 20.6% of organizations were reportedly able to restore data from backups, and in 59 attacks (15.8%) there was evidence that stolen data had been published.

The strongest outcome study links attack dates to Medicare claims. Neprash, McGlave and Nikpay, in a paper published in 2026, found that attacks reduced hospital volume by 17% to 24% in the first week, recovering within three weeks, and that among patients already admitted when an attack began, in-hospital mortality rose by 34% to 38%.¹¹ That is a relative increase among Medicare inpatients; the abstract does not give the baseline rate. A companion analysis of Medicare fee-for-service volume found first-week falls of 14.7% in inpatient admissions, 35.3% in outpatient visits and 10.0% in emergency visits at rural hospitals, effects the authors describe as comparable to those at urban hospitals, but with travel time and distance to the nearest unaffected hospital four to seven times greater.¹²

The harm spreads. Dameff and colleagues compared the emergency departments of an unaffected academic health system before, during and after a month-long ransomware attack on a neighboring health care delivery organization in 2021, across 19,857 visits.¹³ During the attack, mean daily census rose from 218.4 to 251.4, ambulance arrivals from 1,741 to 2,354, patients leaving without being seen from 158 to 360, median waiting-room time from 21 to 31 minutes, and length of stay for admitted patients from 614 to 822 minutes. Stroke code activations rose from 59 to 102 and confirmed strokes from 22 to 47. The authors conclude that such attacks should be treated as disasters requiring coordinated regional planning.

WHAT THE OUTCOME STUDIES DO NOT SHOW

Every outcome study here is of hospitals or emergency departments. None measures what an attack on an ambulatory practice does to its patients, and a mortality effect among admitted inpatients does not translate into an office setting. What does carry over is mechanism: care that depends on the record slows or stops when the record does, and patients go elsewhere.

6 What the rules require today, and what the 2025 proposal would add

A ransomware attack is presumed to be a reportable breach. OCR's 2016 guidance treats the encryption of protected information by ransomware as an acquisition, and so a disclosure the Privacy Rule does not permit.¹⁴ Notification follows unless the entity demonstrates a low probability of compromise under the four-factor assessment in the breach definition.^{2,14} The exception is data the entity had itself encrypted to HHS's standard, which is no longer "unsecured", although OCR cautions that further analysis may still be needed. A business associate must notify the covered entity within 60 days of discovery,² which is how a practice learns of a breach in a vendor's system.

The Security Rule as it reads in September 2026 requires a risk analysis and risk management, a security awareness and training program, and a contingency plan with three required elements: a data backup plan, a disaster recovery plan and an emergency mode operation plan.¹⁵ Testing and revising the contingency plan is "addressable", as is encryption. The authentication standard requires procedures to verify that a person seeking access is the one claimed; the text does not mention multifactor authentication.

OCR proposed to change that on 6 January 2025.¹⁶ The proposal would make all implementation specifications required, with limited exceptions, and would require multifactor authentication and encryption of electronic protected health information at rest and in transit, each with limited exceptions; a technology asset inventory and network map reviewed at least every 12 months; written procedures to restore certain systems and data within 72 hours; vulnerability scanning at least every six months and penetration testing at least every 12 months; network segmentation; separate technical controls for backup and recovery; an annual compliance audit; and annual written verification from business associates that they have deployed the required technical safeguards. Comments closed on 7 March 2025.

None of this is in force. The Spring 2025 Unified Agenda placed the rule at the final rule stage with final action expected in May 2026; the current agenda moved it to long-term actions, with final action projected for July 2027.¹⁷ The Code of Federal Regulations, current as of 24 September 2026, still carries the existing structure of required and addressable specifications.¹⁵

Enforcement runs through the risk analysis

OCR's ransomware enforcement has repeatedly turned on a requirement already in force. In April 2025 it settled with a small New York neurology practice for \$25,000 after a December 2020 attack encrypted its network and all of its electronic protected information, potentially affecting 6,800 people; the potential violation was failure to conduct an accurate and thorough risk analysis.¹⁸ By April 2026 OCR described 19 completed ransomware investigations and 13 in its Risk Analysis Initiative.¹⁹ A 2021 amendment to the HITECH Act requires the Secretary, when determining fines, audit scope and other remedies, to consider whether an entity had recognized security practices in place for the prior 12 months, including

approaches issued under section 405(d) of the Cybersecurity Act of 2015; a lack of such practices cannot be used to increase fines or audits.²⁰ That is the legal weight of the voluntary 405(d) practices discussed below.²¹

Tennessee's breach statute adds little for a covered practice. The statute, T.C.A. § 47-18-2107, defines personal information by Social Security, driver license and financial account numbers, not medical information, and as amended it does not apply to an information holder subject to HIPAA.²² For a HIPAA-covered practice the federal rule is the operative notification obligation.

7 Which controls have evidence, and how much

Federal guidance converges on a short list: multifactor authentication, offline and tested backups, prompt remediation of known vulnerabilities, incident planning and vendor security requirements, each named in one or more of the 405(d) practices for small organizations, the federal #StopRansomware guide and HHS's voluntary Cybersecurity Performance Goals.^{21,23,24} The evidence behind each item is thinner than the agreement (Table 2).

TABLE 2

Common ransomware controls: what the rule requires now, what the 2025 proposal would require, and the evidence located for this review. A dash means the proposal's fact sheet lists no specific change.

Control	Security Rule, Sept. 2026	2025 proposal	Evidence located
Multifactor authentication	Not named; authentication standard only ¹⁵	Required, limited exceptions ¹⁶	Vendor-authored observational analysis; case evidence ^{6,25}
Backups and restoration	Backup plan required; testing addressable ¹⁵	Separate backup controls; 72-hour restoration procedures ¹⁶	Descriptive only: 20.6% restored from backup ⁵
Vulnerability management	Implied by risk management ¹⁵	Scans every 6 months; penetration test every 12 ¹⁶	Guidance only ²³
Awareness training	Program required ¹⁵	—	RCT: little or no effect on phishing failure ²⁶
Business associate assurance	Contract requiring compliance and incident reporting ¹⁵	Annual written verification ¹⁶	None on outcomes; exposure data only ¹
Downtime procedures	Emergency mode operation plan required ¹⁵	—	Safety-event reports; guidance ^{27,28}

Multifactor authentication, and a number that is not a measurement

The case evidence is strong: the Change Healthcare attack began at a remote-access portal without it,⁶ and OCR's 2024 report states that its investigations often found a regulated entity had implemented an authentication solution such as multifactor authentication only after a breach.¹ The figure usually attached to it is not a study. The widely repeated 99.9% appears in a 2019 Microsoft marketing post

stating that it “can block over 99.9 percent of account compromise attacks”, with no method given for the figure.²⁹ The closest thing to a measurement located for this review is a 2023 preprint by Microsoft researchers, who analyzed Azure Active Directory accounts showing suspicious activity and estimated that multifactor authentication reduced the risk of compromise by 99.22% overall and 98.56% where credentials had leaked, with authenticator apps outperforming SMS.²⁵ It is vendor-authored, not peer-reviewed, and measures account takeover in one identity service rather than ransomware in health care. The sources agree on direction. The size of the effect for a practice has not been measured.

Backups that have never been restored

Only about one attacked organization in five was reported to have restored from backup, and the likelihood declined over 2016 to 2021.⁵ Guidance converges on offline, encrypted backups tested by restoration: the federal ransomware guide says so directly,²³ the federal contingency-planning guide recommends backup media separated from normal storage, for example by an air gap, with complete restores tested optimally monthly,²⁸ and the 405(d) volume tells small practices to require offline, offsite, encrypted backups of any prospective managed-service provider.²¹ The current rule requires a backup plan but makes testing addressable,¹⁵ so a backup that has never been restored can satisfy its letter. No controlled study comparing outcomes by backup practice was located.

Training, the one control with a trial located

Ho and colleagues ran an eight-month randomized controlled experiment with ten simulated phishing campaigns sent to more than 19,500 employees of a large health care organization.²⁶ They found no significant relationship between recent completion of annual awareness training and failing a simulation; the absolute difference in failure rates between users who received embedded training and those who did not was extremely low across training content; most users spent minimal time on the material; and for some content, completing more training was associated with a higher likelihood of failing later. The rule requires a training program,¹⁵ and that requirement stands. The trial does not test other controls; it does weaken the case for making staff vigilance a practice’s primary defense.

For vulnerability management and vendor assurance, nothing beyond guidance and exposure data was located. The federal guide prioritizes patching internet-facing systems and known exploited vulnerabilities;²³ the voluntary goals include vendor cybersecurity requirements and third-party incident reporting.²⁴ Both are reasonable. Neither has been evaluated against outcomes.

8 Downtime is a clinical-safety control, not an IT one

The harms measured in section 5 are effects of lost systems, not of lost data. The Security Rule already requires an emergency mode operation plan,¹⁵ but the specification is written around continuing the business processes that protect electronic information, not around continuing care. The safety evidence is

sparse and consistent. Larsen and colleagues found 76 reports, in a database of 80,381 patient safety events, that explicitly described a safety event during electronic record downtime; 48.7% involved laboratory orders and results and 14.5% medication ordering and administration.²⁷

The federal SAFER contingency-planning guide turns this into testable practice.²⁸ It recommends paper forms sufficient for at least 8 hours of care in each patient care area, a read-only copy of the record updated optimally hourly and printable, a process for entering and reconciling paper documentation after recovery, unannounced downtime drills at least once a year, simulated ransomware recovery drills, and a way to announce downtime that does not run on the same infrastructure as the record. These are recommendations, not requirements.

Several properties follow for any electronic record a small practice depends on: a current, read-only copy of the information needed to see patients safely, including schedules, medication lists and allergies, that survives the loss of the vendor; claims submission that does not depend on a single clearinghouse that cannot be replaced within days; multifactor authentication on every remote path into the system, including the vendor's own support access; backups segregated from production, with restoration tested and recorded; and a vendor obligation to report an incident to the practice that is specific enough to act on.

9 What survives

Five statements are supported. Hacking dominates the federal breach record, at 81% of large breach reports in both 2023 and 2024.^{1,3} By people affected, the exposure is concentrated in business associates, 85% of individuals in 2024, and a single clearinghouse attack accounts for most of that year.^{1,7} Clinics are the most commonly attacked delivery organizations.⁵ Attacks reduce hospital volume and raise in-hospital mortality among patients already admitted, and push load onto neighboring hospitals.^{11,12,13} A vendor outage can drain a small practice's cash within weeks, on survey evidence that cannot size the effect.⁹

Three are not supported. No study located for this review measures patient outcomes when an ambulatory practice is attacked. No controlled study in health care located for this review estimates what multifactor authentication or tested backups prevent, although nothing located contradicts them. And the stronger Security Rule proposed in January 2025 is not law; its final action is projected for July 2027.¹⁷

What would settle the open questions is mostly data collection: a ransomware field in OCR reporting, as Jiang and colleagues propose;⁴ claims-based estimates of practice revenue around the Change outage; and outcome studies that compare organizations by backup and authentication practice rather than by whether they were attacked. Until then, the defensible position for a small practice is modest. The controls with the best case support are unglamorous, the control that depends on vigilance has trial evidence of little effect, and the largest recent exposure came from a vendor the practice could not see into.

REFERENCES

Entries 5, 11, 12, 13 and 26 are the peer-reviewed studies that carry the argument on harm and on controls, entry 4 is the peer-reviewed analysis of the breach portal, and entries 1 and 3 are OCR's own counts. Entries 2, 14, 15, 16, 20 and 22 are regulation, guidance, a proposed rule that is not in force (its status is from entry 17) and statute, and entries 21, 23, 24 and 28 are voluntary federal guidance; all are cited for what they say, not as evidence that anything works. Entries 6 and 8 are the attacked company's own statements, entry 9 is an informal self-selected survey, entry 25 is a vendor-authored preprint and entry 29 is a vendor marketing post. Entry 22 was read from an unofficial reproduction of the Tennessee Code because the official site could not be retrieved.

1. U.S. Department of Health and Human Services, Office for Civil Rights. *Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Year 2024*. [hhs.gov](https://www.hhs.gov) GOVERNMENT REPORT
2. 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, §§ 164.400–164.414, including the definition of breach at § 164.402 and notification timing at §§ 164.404(b), 164.408 and 164.410(b) (eCFR, current as of Sept. 24, 2026). [ecfr.gov](https://www.ecfr.gov) REGULATION
3. U.S. Department of Health and Human Services, Office for Civil Rights. *Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Year 2023*. [hhs.gov](https://www.hhs.gov) GOVERNMENT REPORT
4. Jiang JX, Ross JS, Bai G. *Ransomware Attacks and Data Breaches in US Health Care Systems*. JAMA Network Open. 2025;8(5):e2510180. [doi:10.1001/jamanetworkopen.2025.10180](https://doi.org/10.1001/jamanetworkopen.2025.10180) CROSS-SECTIONAL
5. Neprash HT, McGlave CC, Cross DA, et al. *Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021*. JAMA Health Forum. 2022;3(12):e224873. [doi:10.1001/jamahealthforum.2022.4873](https://doi.org/10.1001/jamahealthforum.2022.4873) COHORT
6. Witty A. *Testimony of Andrew Witty, Chief Executive Officer, UnitedHealth Group*. U.S. Senate Committee on Finance, hearing *Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next*, May 1, 2024. [finance.senate.gov](https://www.finance.senate.gov) INDUSTRY STATEMENT
7. U.S. Department of Health and Human Services, Office for Civil Rights. *Change Healthcare Cybersecurity Incident Frequently Asked Questions*. Content last reviewed Aug. 13, 2025. [hhs.gov](https://www.hhs.gov) GOVERNMENT REPORT
8. UnitedHealth Group. *UnitedHealth Group Reports 2024 Results*. Earnings release, Jan. 16, 2025, Exhibit 99.1, SEC EDGAR. [sec.gov](https://www.sec.gov) INDUSTRY STATEMENT

9. American Medical Association. *Change Healthcare cyberattack impact*. Informal survey of the Federation of Medicine, open Mar. 26–Apr. 3, 2024 (ama-assn.org); follow-up survey open Apr. 19–24, 2024 (ama-assn.org). SURVEY
10. Centers for Medicare & Medicaid Services. *CMS Preparing to Close Program that Addressed Medicare Funding Issues Resulting from Change Healthcare Cyber-Attack*. Press release, June 17, 2024. cms.gov GOVERNMENT REPORT
11. Neprash H, McGlave C, Nikpay S. *Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients*. American Economic Journal: Economic Policy. 2026;18(1):256–281. doi:10.1257/pol.20240594 QUASI-EXPERIMENTAL
12. Neprash HT, McGlave CC, Rydberg K, et al. *What happens to rural hospitals during a ransomware attack? Evidence from Medicare data*. The Journal of Rural Health. 2024;40(4):728–737. doi:10.1111/jrh.12834 QUASI-EXPERIMENTAL
13. Dameff C, Tully J, Chan TC, et al. *Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US*. JAMA Network Open. 2023;6(5):e2312270. doi:10.1001/jamanetworkopen.2023.12270 COHORT
14. U.S. Department of Health and Human Services, Office for Civil Rights. *Fact Sheet: Ransomware and HIPAA*. July 11, 2016. hhs.gov GUIDANCE
15. U.S. Department of Health and Human Services. *Security Standards for the Protection of Electronic Protected Health Information*: administrative safeguards, technical safeguards and business associate contracts. 45 C.F.R. §§ 164.308, 164.312, 164.314 (eCFR, current as of Sept. 24, 2026). ecfr.gov REGULATION
16. U.S. Department of Health and Human Services, Office for Civil Rights. *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; with the accompanying fact sheet, *HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information* (hhs.gov). PROPOSED RULE
17. Office of Information and Regulatory Affairs. *HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information*, RIN 0945-AA22. Unified Agenda entries: Spring 2025 (Final Rule Stage; final action 05/2026) and 2026 (Long-Term Actions; final action 07/2027). reginfo.gov GOVERNMENT REPORT
18. U.S. Department of Health and Human Services, Office for Civil Rights. *HHS Office for Civil Rights Settles HIPAA Ransomware Cybersecurity Investigation with Neurology Practice*. Press release, Apr. 25, 2025. hhs.gov GOVERNMENT REPORT

19. U.S. Department of Health and Human Services, Office for Civil Rights. *HHS' Office for Civil Rights Settles Four HIPAA Security Rule Ransomware Investigations*. Press release, Apr. 23, 2026. [hhs.gov](https://www.hhs.gov) GOVERNMENT REPORT
20. United States Congress. *Public Law 116-321*, amending the HITECH Act to add § 13412, *Recognition of security practices*. Approved Jan. 5, 2021. [govinfo.gov](https://www.govinfo.gov) STATUTE
21. HHS 405(d) Task Group. *Technical Volume 1: Cybersecurity Practices for Small Healthcare Organizations*. Health Industry Cybersecurity Practices, 2023 edition. hhscyber.hhs.gov GUIDANCE
22. Tennessee General Assembly. *Release of personal consumer information*. Tenn. Code Ann. § 47-18-2107 (Acts 2005, ch. 473; 2016, ch. 692; 2017, ch. 91). Text read from the Justia reproduction of the 2025 Tennessee Code; the official legislative site could not be retrieved. law.justia.com STATUTE
23. Cybersecurity and Infrastructure Security Agency, Multi-State Information Sharing and Analysis Center, National Security Agency, Federal Bureau of Investigation. *#StopRansomware Guide*. Updated Sept. 2023. cisa.gov GUIDANCE
24. U.S. Department of Health and Human Services. *HPH Cybersecurity Performance Goals*. Voluntary goals for the Healthcare and Public Health sector, ten essential and ten enhanced; released Jan. 24, 2024 (release date as reported by Health-ISAC; the HHS page is undated). hhscyber.hhs.gov GUIDANCE
25. Meyer LA, Romero S, Bertoli G, et al. *How effective is multifactor authentication at deterring cyberattacks?* arXiv. 2023. [arXiv:2305.00945](https://arxiv.org/abs/2305.00945). Authors from Microsoft. PREPRINT
26. Ho G, Mirian A, Luo E, et al. *Understanding the Efficacy of Phishing Training in Practice*. 2025 IEEE Symposium on Security and Privacy (SP). 2025:37–54. [doi:10.1109/SP61157.2025.00076](https://doi.org/10.1109/SP61157.2025.00076) RCT
27. Larsen E, Fong A, Wernz C, et al. *Implications of electronic health record downtime: an analysis of patient safety event reports*. Journal of the American Medical Informatics Association. 2018;25(2):187–191. [doi:10.1093/jamia/ocx057](https://doi.org/10.1093/jamia/ocx057) CROSS-SECTIONAL
28. Flanagan T, Singh H, Sittig DF. *SAFER for EHR Resilience: Contingency Planning*. Assistant Secretary for Technology Policy / Office of the National Coordinator for Health Information Technology; dated Aug. 2024, issued with the 2025 update of the SAFER Guides. healthit.gov GUIDANCE
29. Maynes M. *One simple action you can take to prevent 99.9 percent of attacks on your accounts*. Microsoft Security blog, Aug. 20, 2019. microsoft.com INDUSTRY STATEMENT

RELATED PAPERS

HIPAA and the model

What a business associate agreement requires of a vendor, and what it leaves out

Automation in the revenue cycle

The claims pipeline that a clearinghouse outage interrupts

Tamper-evident clinical records

Showing that a restored record has not been altered, and the limits of that proof