BRIDGHAM TECHNOLOGY INSTITUTE
BTI WORKING PAPER 324-26

The Business Associate Share of Health Data Breaches: Evidence From HHS Breach Reports to Congress, 2020 to 2024

Bridgham Technology Institute

This work is made available under the rights statement In Copyright - Educational Use Permitted
https://rightsstatements.org/page/InC-EDU/1.0/
Raleigh, NC: Bridgham Technology Institute, November 2026.

Electronic copy available at: https://bridghaminstitute.com/research/working-papers/324-26

The Business Associate Share of Health Data Breaches: Evidence From HHS Breach Reports to Congress, 2020 to 2024

Bridgham Technology Institute*

November 2026

Abstract: Health care providers and the other entities covered by HIPAA hand protected health information to vendors that the law calls business associates. We examine how much of the exposure in large HIPAA breaches was reported by those vendors, using the five annual reports from the HHS Office for Civil Rights to Congress for calendar years 2020 to 2024. The reports count 3,286 breaches affecting 500 or more individuals and 472,653,243 individuals affected, where an individual is counted once per report and so can be counted more than once. Business associates filed 533 of the reports (16.2%), and those reports account for 297,513,677 individuals (62.9%). One 2024 event of about 192 million individuals carries much of that weight; with it removed the share is 37.6%, and in no year from 2020 to 2024 did the share fall below 25.7%. A breach reported by a business associate affected on average 8.9 times as many individuals as one reported by a provider, or 3.1 times with the 2024 event removed. Hacking or IT incidents account for 95.7% of individuals affected over the period. Because each breach is counted under the entity that filed it, the measure most likely understates the part of exposure that sits with vendors. These results suggest that the records held by business associates are a large part of a health care organization's exposure, at a time when a proposed update to the HIPAA Security Rule, now estimated for final action in July 2027, would require written verification of business associate safeguards at least once every 12 months.

Keywords: HIPAA Security Rule, business associates, breach reports, protected health information, third-party risk, HHS Office for Civil Rights, health care providers
JEL codes: I18, K23

* Bridgham Technology Institute is a division of Bridgham Cyber, LLC, Raleigh, NC. Contact: headofresearch@bridghamcyber.com.

1. Introduction

A health care group that holds patient records also hands a share of them to others: billing and coding firms, electronic health record hosts, transcription services, IT providers and claims processors, and clearinghouses acting for the group. Under HIPAA, a vendor that handles protected health information for a covered entity is a business associate, bound by a business associate agreement to safeguard the electronic protected health information it receives.[1]

The board of such a group faces a practical question: how much of the organization's breach exposure sits with its vendors? The record that answers the question at the level of the sector is public. The HHS Office for Civil Rights (OCR) reports to Congress each year on breaches of unsecured protected health information, under section 13402 of the HITECH Act.[2] Each report counts the breaches affecting 500 or more individuals, the number of individuals affected, and the type of entity that filed each report.

In this paper, we examine the five most recent reports, for calendar years 2020 to 2024,[2–6] and combine them into one measure: the share of individuals affected by large breaches whose breach was reported by a business associate and not by a health care provider, health plan or clearinghouse. We report two companion figures beside it, the business associate share of reports and the average size of a business associate report relative to a provider report.

We document three main findings. First, business associates file a small share of reports and account for a much larger share of individuals. They filed 533 of the 3,286 large breach reports (16.2%), and those reports account for 297,513,677 of the 472,653,243 individuals affected (62.9%). Second, one event carries much of that weight, and the pattern holds without it. With the 2024 event of about 192 million individuals removed, the share is 37.6%, and the share in each single year ranges from 25.7% in 2021 to 85.2% in 2024. Third, the breaches reported by business associates are the large ones. A business associate report affected on average 558,187 individuals, against 62,892 for a provider report, a ratio of 8.9 that falls to 3.1 with the 2024 event removed. Across all filers, hacking or IT incidents account for 95.7% of the individuals affected over the period.

These findings are counts of breach reports and of individuals per report. They are not counts of incidents or of unique people. OCR counts an individual once in each report, so one person can be counted more than once across reports and years. Each breach is also counted under the entity that filed it. A breach at a vendor that the provider files counts as a provider breach, so the measure most likely understates the exposure that sits with vendors. The measure describes the sector and does not describe any single organization.

The question is timely. In January 2025 HHS proposed a revision of the HIPAA Security Rule.[1] Among other changes, the proposal would require a business associate to verify its technical safeguards to each covered entity at least once every 12 months, through a written analysis by a subject matter expert and a written certification, and to notify the covered entity within 24 hours of

activating its contingency plan.[7] The current Unified Agenda entry for the rule lists final action for July 2027.[8] A health care group preparing for that rule, for an OCR audit, or for a cyber insurance renewal that asks about vendor oversight needs to know how large the vendor share has been.

The paper proceeds as follows. Section 2 describes the OCR reports and the breaches they cover. Section 3 defines the measure, its weights and the assumptions behind it. Section 4 presents the results. Section 5 discusses what the results mean for a health care group and for the proposed Security Rule. Section 6 states the limitations, and Section 7 concludes.

2. Data

2.1. Sources

Our data are the five OCR annual reports to Congress on breaches of unsecured protected health information, for calendar years 2020, 2021, 2022, 2023 and 2024.[2–6] For breaches affecting 500 or more individuals, each report gives the number of reports and the number of individuals affected by entity type (health care provider, health plan, business associate, health care clearinghouse) and by type of breach (hacking or IT incident, unauthorized access or disclosure, theft, loss, improper disposal). We read the figures from each report and checked them by summing the four entity-type rows against the printed total, for both reports and individuals. All ten sums match.

OCR counts individuals per breach report. The same person can appear in more than one report in a year and across years, so the totals in this paper are counts of individuals per report and are not counts of unique people.

We use no client data, survey or proprietary dataset, and Bridgham Technology Institute has collected no breach data of its own for this paper. Every number in Section 4 can be rebuilt from Tables 1 and 3, and every number in those tables can be found in the cited reports.

2.2. Scope

Table 1 reports the large breach reports and the individuals affected in each year, by filing entity. We use only breaches affecting 500 or more individuals, which are the breaches OCR investigates in every case.[2] Breaches affecting fewer than 500 individuals are reported to OCR after the end of each calendar year. In 2024 there were 74,299 such reports, affecting about 340,618 individuals in total, or about 0.1% of the individuals affected by large breaches that year.[2]

Year	All reports	Individuals	Business associate reports	Business associate individuals	Provider reports	Provider individuals
2020	656	37,641,403	78	10,938,223	504	20,287,314
2021	609	37,182,558	77	9,554,023	437	24,389,630
2022	626	41,747,613	120	14,580,712	425	24,481,253
2023	732	113,173,613	152	55,519,648	461	43,048,365
2024	663	242,908,056	106	206,921,071	505	34,456,670
2020 to 2024	3,286	472,653,243	533	297,513,677	2,332	146,663,232

Table 1: Large HIPAA Breach Reports (500 or More Individuals) by Filing Entity, 2020 to 2024. Source: OCR annual reports to Congress for each calendar year.

3. Measure and Assumptions

3.1. The Measure

Our main measure is the business associate share of individuals affected, B. It is the number of individuals affected by large breaches filed by business associates divided by the number of individuals affected by all large breaches, pooled over the five years:

B = (sum over years of individuals in business associate reports) / (sum over years of individuals in all reports)

We report two companion measures. The report share, R, is the number of business associate reports divided by all reports. The size ratio, K, is the average number of individuals per business associate report divided by the average number per provider report.

3.2. Weights

Pooling weights each year by the number of individuals affected in that year. The resulting year weights are 8.0% (2020), 7.9% (2021), 8.8% (2022), 23.9% (2023) and 51.4% (2024). The heavy weight on 2024 is a property of the data: one event in that year affected about 192 million individuals. Appendix A gives the measure under equal year weights, with the median year, with that event removed, and over shorter periods.

3.3. Assumptions

The measure rests on five assumptions. First, we use the counts as printed. OCR notes that individual counts are approximate, because some filers could not state an exact number.[6]

Second, each breach is assigned to the entity type that filed the report, which is how OCR classifies it.[2] A covered entity keeps the duty to notify affected individuals and may delegate that duty to its business associate by agreement,[2] so a breach that occurred at a business associate can be filed by either party. A breach at a vendor that is filed by the provider counts here as a provider breach.

Third, we make no adjustment for one vendor event that produces several reports, for example when many covered entities each file for the same incident at a shared vendor.

Fourth, we place the 2024 event of about 192 million individuals in the business associate row. The 2024 report describes it as the compromise of a health care clearinghouse's servers,[2] while the same report's entity-type table assigns 226,822 individuals in total to clearinghouses and 206,921,071 to business associates.[2] Only the business associate row is large enough to hold it. We therefore take the event as filed by a business associate, and Appendix A shows the measure without it. HHS records that the filer's own estimate rose from about 190 million (January 2025) to about 192.7 million (July 2025);[9] Appendix A removes each of 190.0, 192.0 and 192.7 million.

Fifth, breaches not reported to OCR are outside the data. We make no estimate of them.

4. Results

4.1. The Pooled Share

Table 2 reports each year and the pooled result. From 2020 to 2024, business associates filed 533 of 3,286 large breach reports (R = 16.2%). Those 533 reports account for 297,513,677 of 472,653,243 individuals affected (B = 62.9%). A business associate report affected on average 558,187 individuals, against 62,892 for a provider report (K = 8.9). Figure 1 shows the share of individuals in each year, with the business associate share of reports marked within each bar.

Year	Report share (R)	Individuals share (B)	Individuals per BA report	Individuals per provider report
2020	11.9%	29.1%	140,234	40,253
2021	12.6%	25.7%	124,078	55,812
2022	19.2%	34.9%	121,506	57,603
2023	20.8%	49.1%	365,261	93,380
2024	16.0%	85.2%	1,952,086	68,231
2020 to 2024 pooled	16.2%	62.9%	558,187	62,892
Pooled, 2024 event removed	16.2%	37.6%	197,962	62,892

Table 2: Business Associate Share of Large Breach Reports and of Individuals Affected, by Year and Pooled.

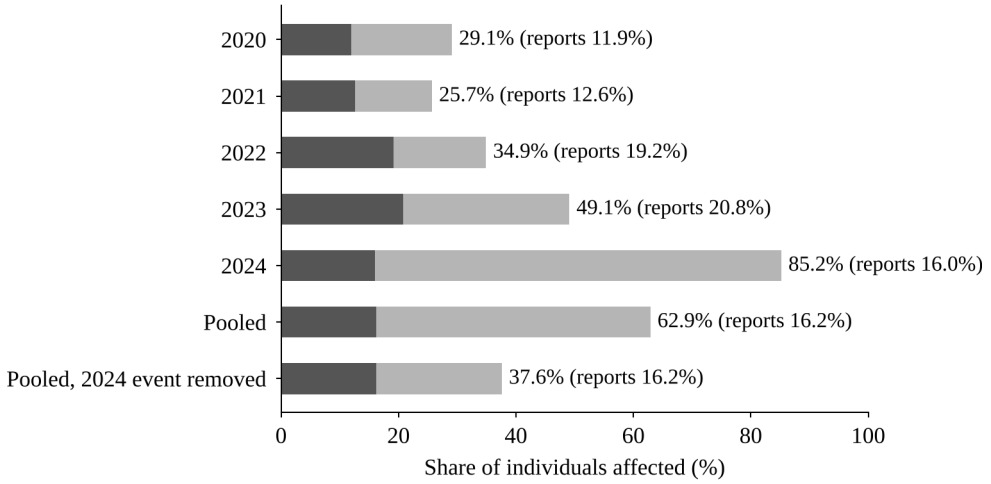


Figure 1: Business Associate Share of Individuals Affected by Large HIPAA Breaches, 2020 to 2024. The darker segment is the business associate share of reports in the same year.

4.2. The Effect of One Event

With the 2024 event of about 192 million individuals removed, business associate reports account for 105,513,677 of 280,653,243 individuals (37.6%), and the size ratio falls from 8.9 to 3.1. The share in each single year from 2020 to 2023, none of which contains that event, ranges from 25.7% to 49.1%. Business associates file a small share of reports and account for a much larger share of individuals in every year. The individuals share exceeds the report share by 13.1 percentage points in 2021, the narrowest year, and by 69.2 points in 2024, the widest.

4.3. How the Breaches Occurred

Table 3 reports hacking or IT incidents in each year. These incidents account for 2,489 of 3,286 large reports (75.7%) and 452,093,479 of 472,653,243 individuals (95.7%) over the five years. In 2024 the share of individuals in hacking or IT incidents was 99.5%, and 98% of individuals were affected by breaches located on network servers.[2] In the lessons-learned section of its 2024 report, OCR lists the Security Rule areas that breach reports and investigations show as needing improvement: risk analysis, risk management, review of information system activity, access control and authentication, including single-factor remote access.[2]

Year	Hacking reports	Share of reports	Hacking individuals	Share of individuals
2020	444	67.7%	34,265,326	91.0%
2021	459	75.4%	35,264,773	94.8%
2022	462	73.8%	32,255,597	77.3%
2023	590	80.6%	108,725,761	96.1%
2024	534	80.5%	241,582,022	99.5%
2020 to 2024	2,489	75.7%	452,093,479	95.7%

Table 3: Hacking or IT Incidents in Large HIPAA Breaches, 2020 to 2024.

5. Discussion

Our results describe the sector and do not describe any single health care group. They show that, over five years, most individuals whose records were exposed in large HIPAA breaches were exposed in breaches filed by vendors, and that the average vendor breach was several times larger than the average provider breach. The likely reason is structural: a single clearinghouse, billing firm or hosting provider holds records for many covered entities at once, so one compromise reaches the patients of all of them. For a health care group, these results suggest that the records held by its business associates are a large part of its exposure, and that a contract alone does not show whether those records are protected.

The vendor share in health care can be set beside a figure for all sectors. The 2025 Verizon Data Breach Investigations Report, across 12,195 confirmed breaches in all sectors, reports that the share of breaches with a third party involved doubled from 15% to 30%.[10] That figure counts breaches and not individuals, and it uses a different definition of involvement, so it is not directly comparable with B. It is closest to R, the report share, which in our data was 16.2% over five years and 16.0% in 2024. The health care data adds what a count of breaches cannot show: the vendor breaches are the large ones.

The proposed Security Rule bears on the same vendor relationships. The current Security Rule already requires a covered entity to have business associate agreements that oblige its business

associates to safeguard electronic protected health information.[1] The January 2025 proposal would add a recurring check: written verification, at least once every 12 months, that each business associate has deployed the required technical safeguards, supported by a written analysis by a subject matter expert and a written certification that the analysis is accurate.[7] It would also require a business associate to notify the covered entity no later than 24 hours after activating its contingency plan.[7] The current Unified Agenda entry moves the estimated date of final action to July 2027, from May 2026 in the Spring 2025 edition.[8] The content of a final rule may differ from the proposal.

The results point to three steps a health care group may take before any final rule. The first is an inventory of business associates ranked by the volume of records each holds. The second is a written request to the largest of them for evidence of the safeguards OCR lists as needing improvement, in particular risk analysis and multi-factor authentication for remote access.[2] The third is a contract term that sets a notice period for incidents and for activation of contingency plans.

6. Limitations

Our analysis has six limitations. First, the filing entity is a proxy for the place where a breach occurred. Each breach is counted under the entity that filed it. Breaches that occurred at a vendor but were filed by the provider count as provider breaches, which most likely makes B an understatement of the share of exposure held by vendors. The opposite case, a business associate filing for a breach that occurred at a covered entity, is possible but is not the usual direction of the duty to notify.

Second, one event carries much of the weight. The 2024 event of about 192 million individuals makes up 40.6% of all individuals in the five-year data. We give the measure with and without it, and we test its removal at 190.0 and 192.7 million, which gives a share between 37.4% and 38.0%.

Third, the data count reports and not incidents. One incident at a shared vendor can produce many reports, filed by many covered entities. This multiple filing inflates report counts for providers and lowers R. Within a single report each individual is counted once; the same individual can still appear in more than one report.

Fourth, some counts are approximate. OCR states that some individual counts are approximate.[6] Rounding in the source tables does not affect the totals we use, which are printed to the individual.

Fifth, the measure covers large breaches only. Breaches affecting fewer than 500 individuals are outside it, and in 2024 they made up about 0.1% of individuals affected.[2] Sixth, the period is five years. The years 2020 to 2024 are the span of the five most recent reports, and we had not read the 2025 report for this paper.

7. Conclusion

Health care groups share patient records with business associates, and the federal breach reports show how much of the reported exposure those vendors have carried. We measure the business associate share of large HIPAA breaches in the five OCR reports to Congress for 2020 to 2024. Business associates filed 16.2% of large breach reports and accounted for 62.9% of the individuals affected. With the single largest event removed the share is 37.6%, and in no year did it fall below 25.7%.

A breach filed by a business associate affected, on average, between 3.1 and 8.9 times as many individuals as a breach filed by a provider, depending on whether that event is counted. Because breaches are counted under the filing entity, these figures most likely understate the vendor share.

Although these counts describe the sector and not any one organization, they do show where the exposure has been reported. For a health care group, the evidence suggests that the records held by business associates are a large and measurable part of its own exposure, and that preparing now for the annual written verification the proposed Security Rule would require may be worthwhile.

Appendix A: Sensitivity of the Measure

Table A.1 reports the business associate share of individuals under each alternative weighting and period. Removing one event leaves the report share unchanged, because that event is one report among 3,286.

Specification	Individuals share (B)	Report share (R)	Size ratio (K)
Baseline: pooled, 2020 to 2024, weighted by individuals	62.9%	16.2%	8.9
Pooled, 2024 event of about 192 million removed	37.6%	16.2%	3.1
Pooled, 2024 event removed at 190.0 million	38.0%	16.2%	3.2
Pooled, 2024 event removed at 192.7 million	37.4%	16.2%	3.1
Equal weight per year (mean of annual shares)	44.8%	16.1%	n/a
Median year (2022)	34.9%	19.2%	2.1
Pooled, 2020 to 2023 only	39.4%	16.3%	3.5
Pooled, 2022 to 2024 only	69.6%	18.7%	10.0
Lowest single year (2021)	25.7%	12.6%	2.2
Highest single year (2024)	85.2%	16.0%	28.6

Table A.1: Business Associate Share of Individuals Affected Under Alternative Specifications.

Across every specification, the business associate share of individuals is at least 13.1 percentage points above the business associate share of reports, and the size ratio is at least 2.1. The level of B depends heavily on whether the 2024 event is counted. The direction of the finding does not.

References

1. U.S. Department of Health and Human Services, Office for Civil Rights. (2025). HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information. Notice of proposed rulemaking. Federal Register, 90 FR 898 (January 6, 2025), RIN 0945-AA22. https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information

2. 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. Totals and entity type, p. 9; breach type, p. 11; location, p. 13; largest breaches, p. 16; under-500 breaches, p. 18; investigations and lessons learned, pp. 27 to 29. https://www.hhs.gov/sites/default/files/breach-report-to-congress-2024.pdf

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. Totals, p. 8; entity type, p. 9; breach type, p. 10. https://www.hhs.gov/sites/default/files/breach-report-to-congress-2023.pdf

4. 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 2022. Totals and entity type, pp. 8 to 9; breach type, p. 10. https://www.hhs.gov/sites/default/files/breach-report-to-congress-2022.pdf

5. 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 2021. Totals, p. 8; entity type, p. 9; breach type, p. 10. https://www.hhs.gov/sites/default/files/breach-report-to-congress-2021.pdf

6. 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 2020. Totals, p. 6, with note on approximate counts; entity type, p. 7; breach type, p. 10. https://www.hhs.gov/sites/default/files/breach-report-to-congress-2020.pdf

7. U.S. Department of Health and Human Services, Office for Civil Rights. (2024). HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information: Fact Sheet. December 27, 2024. https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html

8. Office of Information and Regulatory Affairs. Unified Agenda of Regulatory and Deregulatory Actions, HHS, RIN 0945-AA22, HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information. Edition listed on reginfo.gov as 2026 (publication 202510): Long-Term Actions; NPRM 01/06/2025, 90 FR 898; Final Action 07/00/2027. Spring 2025 edition (publication 202504) for the earlier date. https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202510&RIN=0945-AA22

9. U.S. Department of Health and Human Services, Office for Civil Rights. Change Healthcare Cybersecurity Incident Frequently Asked Questions (updates of January 24, 2025 and July 31, 2025). https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html

10. Verizon. (2025). 2025 Data Breach Investigations Report: Executive Summary (22,052 incidents, 12,195 confirmed breaches). https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

Disclaimer

This report is published by Bridgham Technology Institute for informational and analytical purposes only. It does not constitute investment advice, legal counsel, or a solicitation of any kind. All data are drawn from public HHS reports and one named industry report. No client data, proprietary data or survey data was used, and no organization was contacted. Reproduction or redistribution of this report, in whole or in part, requires attribution to Bridgham Technology Institute. For questions regarding methodology or data, contact headofresearch@bridghamcyber.com.