The State of Compliance Series | Vol. 1, Issue 1

State of Compliance

Q1 2026 Healthcare Breach Review

207 Breaches
15.9M Affected
4 Incidents = 67.6% of Impact
Multi-Source Compilation

PUBLISHED BY
Secure Care Research Institute
Patient Protect LLC

VERSION
1.3 · 2026

Abstract

JEL Classifications: D82, I18, K23, L51

Keywords: HIPAA, healthcare cybersecurity, breach economics, disclosure transparency, risk analysis, Security Rule, business associate risk

This working paper inaugurates the State of Compliance series, a quarterly empirical review of the U.S. healthcare data breach landscape published by the Secure Care Research Institute. The Q1 2026 review draws on the Patient Protect Breach Intelligence Dashboard, a multi-source compilation of HHS Office for Civil Rights breach reporting, state attorney general filings, FTC enforcement actions, CISA advisories, and primary entity disclosures. After deduplication of multi-state filings and exclusion of records outside healthcare-sector scope, the dashboard records 207 unique large healthcare breaches reported between January 1 and March 31, 2026, affecting the protected health information of approximately 15.9 million individuals.

The multi-source compilation is the principal methodological contribution of this paper. The HHS OCR breach portal alone, accessed in late March 2026, recorded 118 breaches for January–February 2026 and only two breach reports for March 2026 against an investigation-pending queue of 978 cases. By the late-April 2026 dashboard export used in this paper, the OCR portal had caught up to 169 deduplicated Q1 records, and the addition of state attorney general filings produced the dashboard's 207-record full-quarter view. The multi-source view exceeds the late-March OCR-only snapshot by approximately 75% and the late-April OCR-only deduplicated count by approximately 22%, demonstrating the empirical lift that multi-source compilation produces over OCR-only reporting in a quarter materially affected by the 43-day federal government shutdown of late 2025.

Three findings frame the period. First, four upstream business associate and platform incidents — TriZetto Provider Solutions (3.43M), QualDerm Partners (3.12M), Healthcare Interactive (3.06M), and Insightin Health (1.14M) — together account for 67.6% of all Q1 2026 affected individuals across just 1.9% of the incident count. The concentration is the sharpest empirical evidence yet of the upstream business-associate aggregation dynamic identified in prior research (Perrin, 2025a). Second, the named-incident record comprises a structurally diverse set of archetypes: platform and business-associate cascades, named-group ransomware, insider exfiltration, offshore data mishandling, publicly-attributed nation-state targeting of medical device infrastructure, and long-latency detection-gap disclosures. Third, the Healthcare Transparency Index gap identified in prior research (Perrin, 2025b) widened modestly across the period. The OCR investigation queue grew to 978 cases as the federal government processed a substantial reporting volume; OCR's March 2026 reporting reflected the cumulative effect of the late-2025 federal shutdown on portal updates; and named-incident detection-to-disclosure intervals ranged from approximately 64 days (Stockton Cardiology, attack to ransomware leak publication) to approximately 195 days (IPPC, attack to individual notification). The findings reflect the structural realities of a large, complex reporting ecosystem operating under significant volume pressure rather than a judgment about regulatory performance.

The quarter also opened a regulatory window. Effective February 16, 2026, OCR's civil enforcement authority over 42 CFR Part 2 substance use disorder records took effect, and OCR began accepting Part 2 breach notifications and complaints through its existing reporting portal. The February 19, 2026 OCR settlement with Top of the World Ranch Treatment Center ($103,000, resolving alleged noncompliance with the risk analysis requirement at 45 CFR §164.308(a)(1)(ii)(A)) signaled continued enforcement of the risk-analysis provision. The 2026 HIPAA Security Rule update (NPRM published December 27, 2024) remains the largest pending regulatory variable, with finalization timing subject to uncertainty following the January 20, 2025 regulatory freeze executive order. The paper applies the Transparency-Adjusted Risk Function (Perrin, 2025b) qualitatively to the Q1 2026 context and concludes with recommendations for covered entities, business associates, and regulators.

Executive Summary

Q1 2026 was not a quiet quarter, but the OCR breach portal alone suggested it was.

The HHS OCR breach portal recorded 46 large healthcare breaches in January 2026 and 63 in February 2026, with affected populations totaling 9,651,076 individuals as of late-March 2026 portal access. The portal recorded only two breach reports for March 2026 against an investigation-pending queue of 978 cases. The Patient Protect Breach Intelligence Dashboard, which compiles healthcare breach data across HHS OCR, fifty state attorney general offices, FTC enforcement records, CISA advisories, and primary entity disclosures, surfaces a materially different picture: 207 unique large healthcare breaches across the full Q1 2026 quarter affecting approximately 15.9 million individuals. The dashboard is the principal data source of this paper. Six observations anchor the period.

1. Four upstream incidents drove 67.6% of all Q1 2026 affected individuals.

TriZetto Provider Solutions (3,433,965 affected), QualDerm Partners (3,117,874), Healthcare Interactive / HCIactive (3,056,950), and Insightin Health (1,144,686) together account for 10,753,475 of the approximately 15.9 million individuals affected by Q1 2026 healthcare breaches in the multi-source dataset. These four incidents represent 1.9% of the period's incident count (4 of 207) and 67.6% of its population impact. All four are upstream business associate or platform-vendor incidents whose downstream notification obligations propagate across hundreds of covered entities.

2. Multi-source compilation surfaces what OCR-only reporting misses.

The HHS OCR breach portal alone, accessed in late March 2026, recorded 118 January–February breaches and only two March 2026 reports. The Patient Protect Dashboard's late-April 2026 export surfaces 207 unique Q1 2026 healthcare breaches after deduplication and healthcare-sector scope filtering, an empirical lift of approximately 75% over the late-March OCR-only snapshot used as the principal comparison baseline. By late-April, the OCR portal itself had caught up to 169 deduplicated Q1 records (a 22% gap that the dashboard's state AG channel additionally fills). The combined lift is concentrated in March 2026, where state attorney general filings (notably Oregon AG) and continued OCR backlog clearance through April 2026 surface incidents that the OCR portal alone had not yet displayed at late-March access.

3. Detection-to-disclosure gaps in named cases remained well above regulatory and sector norms.

Stockton Cardiology: initial phishing December 15, 2025; internal file-access discovery January 17, 2026; public disclosure via GENESIS ransomware leak February 17, 2026 (64 days attack-to-leak-disclosure); California AG report March 20, 2026 (95 days attack-to-formal-report). IPPC: attack September 18-19, 2025; website notice February 27, 2026 (~162 days); individual notification letters April 1, 2026 (~195 days). Healthcare Interactive: attack July 8-12, 2025; OCR placeholder filing September 22, 2025; Oregon AG full disclosure January 7, 2026 (~180 days attack-to-substantive-disclosure). The healthcare sector benchmark remains 93 days (Ponemon Institute, 2024, as cited in Perrin, 2025b), against a 4-business-day SEC finance-sector disclosure requirement.

4. The OCR investigation queue continues to grow as breach volume rises against established enforcement resources.

As of January 31, 2026, 978 healthcare data breaches were under or awaiting OCR investigation, up from 882 at the comparable date in 2025 (a 10.9% year-over-year increase). The growth reflects the well-documented structural reality that breach reporting volume has risen faster than enforcement resourcing across multiple administrations; the 43-day shutdown of late 2025 added incremental pressure to a queue whose growth predates it.

5. The period added a publicly-reported cyberattack on a U.S. medical device manufacturer with open-source nation-state attribution.

The Stryker medical-device cyberattack has been publicly reported and linked in open-source reporting to Iran-affiliated actors. Two attribution caveats apply. First, nation-state attribution in cyber incidents is inherently probabilistic; readers should treat the open-source linkage as a working characterization rather than a finding of fact. Second, the Stryker incident appears in the dashboard via the modeled-threat-signal channel rather than via primary HIPAA breach filing, and is excluded from the deduplicated 207-incident analytical dataset. The incident is referenced in §4.5 because the reporting boundary it illustrates — the gap between HIPAA enforcement (OCR) and medical device cybersecurity oversight (FDA) — is itself diagnostically interesting.

6. The regulatory environment opened two new variables within the period.

Effective February 16, 2026, OCR's civil enforcement authority over 42 CFR Part 2 substance use disorder records took effect, and OCR began accepting Part 2 breach notifications and complaints through its existing reporting portal (TechTarget/HealthITSecurity, 2026; Reed Smith, 2026). The OCR Top of the World Ranch settlement (February 19, 2026) imposed a $103,000 civil money penalty resolving alleged noncompliance with the risk analysis requirement at 45 CFR §164.308(a)(1)(ii)(A) (Hunton Andrews Kurth, 2026). The 2026 HIPAA Security Rule update (NPRM December 27, 2024) remains the largest pending regulatory variable; finalization timing is subject to uncertainty following the January 20, 2025 regulatory freeze executive order.

The pattern across these observations is asymmetry. The attacker-side economic architecture established in prior research (dark-market PHI pricing, AI-amplified fraud yield, multi-year record reusability) was not measured to have changed within Q1 2026, and no factor observed in the period would compress it. The defender-side disclosure and enforcement environment, by contrast, continued to operate under the structural workload pressures documented in prior research, with the late-2025 federal shutdown adding incremental stress to OCR portal reporting cadence in particular. The Transparency-Adjusted Risk Function (Perrin, 2025b) predicts that such a configuration sustains an exploitation window regardless of year-over-year breach counts, and the observed Q1 record is consistent with that prediction. The framework is hypothesis-generating rather than hypothesis-testing; the inference rests on multi-indicator structural reasoning rather than direct empirical measurement, and direct comparison of threat velocity and reporting velocity would require data sources not currently published.

Contents

1. Introduction and Scope

The State of Compliance series exists because quarterly breach reporting in U.S. healthcare is fragmented across at least seven authoritative sources — the HHS Office for Civil Rights breach portal, fifty state attorney general offices, Federal Trade Commission enforcement data, CISA vulnerability advisories, CMS enforcement records, community intelligence channels, and modeled threat signals — and because the resulting picture is rarely assembled in one place with academic rigor and independent funding. The Patient Protect Breach Intelligence Dashboard unifies these sources into twelve analytical views and is the empirical foundation of this series (Patient Protect Breach Intelligence Dashboard, 2026).

This issue, the inaugural volume, covers the period January 1 through March 31, 2026. It is restricted to U.S. healthcare-sector breaches — covered entities, business associates, and upstream platform vendors whose data products serve healthcare organizations. Adjacent-sector incidents (education, general municipal government, pure financial services, international) are excluded from the analytical set although referenced where they illuminate healthcare dynamics.

A note on data sourcing is appropriate at the outset. The HHS OCR breach portal alone, accessed in late March 2026, listed only two March 2026 breach reports against a trailing five-month monthly average of 46.2 reports — an OCR-only view that would have suggested March was nearly absent from the breach record. The dashboard's multi-source compilation, drawing on state attorney general filings (notably Oregon AG) and continued OCR backlog clearance through late April 2026, surfaces 80 unique March 2026 breaches, demonstrating exactly the empirical gap that OCR-only reporting produces in a quarter materially affected by the 43-day federal shutdown of late 2025. The full-quarter empirical record used in this paper is the dashboard's deduplicated and healthcare-sector-scoped Q1 2026 total of 207 unique breaches affecting approximately 15.9 million individuals; this total may continue to be revised modestly upward as further late-arriving reports propagate through the OCR portal in subsequent quarters.

The purpose of this paper is threefold: to establish the quarterly empirical record for Q1 2026 using the multi-source dashboard, to apply the analytical framework developed in prior Secure Care Research Institute working papers (Perrin, 2025a; Perrin, 2025b) to that record, and to publish recommendations for covered entities, business associates, and regulators that are derived from the data rather than from vendor marketing priorities.

This paper is not a threat intelligence feed, a compliance checklist, or a legal analysis. It does not provide legal advice. It does not rank vendors. It does not reproduce or endorse any commercial compliance methodology. Readers seeking operational compliance guidance are directed to qualified HIPAA counsel.

2. Methodology and Multi-Source Compilation

The Q1 2026 empirical record presented in this paper is drawn from the Patient Protect Breach Intelligence Dashboard, a proprietary multi-source compilation of healthcare breach reporting maintained by Patient Protect LLC (https://patient-protect.com/breachdash). The dashboard ingests breach intelligence from seven primary channels and reconciles them into twelve analytical views. The seven channels are: (1) the HHS Office for Civil Rights breach portal, the regulatory baseline for breaches affecting 500 or more individuals; (2) state attorney general notifications across all fifty states, frequently surfacing incidents weeks before federal reporting; (3) FTC enforcement data, capturing non-HIPAA entities handling health data; (4) CISA vulnerability advisories, contributing infrastructure-level threat signals; (5) CMS enforcement records; (6) crowdsourced community intelligence from healthcare security practitioners; and (7) modeled threat signals derived from cross-source anomaly detection.

For Q1 2026 the principal sources used in this paper are HHS OCR (173 raw breach records, accessed late April 2026) and state attorney general filings (45 raw records, with the largest contributors being Oregon, California, Washington, and Indiana). FTC enforcement actions, CISA advisories, and CMS enforcement records did not contribute new breach incidents to the Q1 2026 dataset; their dashboard contributions during the period were enforcement and advisory records that fall outside the breach-incident scope of this paper. Because some incidents are filed in both OCR and state attorney general channels, the raw counts do not sum to the final deduplicated total. The originating-source attribution for each unique deduplicated incident is described below and detailed in Appendix D.

All incident counts and affected-population figures presented in this paper are derived from publicly available disclosures and may be revised as additional filings, data reviews, and updates are released by the originating entities and their regulators. The empirical record is intentionally treated as provisional rather than final.

Multi-source compilation is methodologically necessary in U.S. healthcare breach analysis because no single channel captures the full breach record in real time. The HHS OCR portal experiences material reporting delays, exemplified by the 43-day federal government shutdown of late 2025, during which no breach reports were added to the portal. State attorney general filings under state breach notification laws (notably the Oregon Consumer Information Protection Act, the California Consumer Privacy Act, and analogous state laws) frequently capture breach disclosures before HHS OCR adds them to its public portal. Initial OCR filings often use placeholder figures of 500 or 501 affected individuals while data reviews remain open; subsequent state-level filings provide the revised affected-population totals before OCR updates the original entry. The Healthcare Interactive incident (§3.2, §4.1) is the clearest Q1 2026 example: the OCR portal carried a 501-individual placeholder while the Oregon AG's January 7, 2026 disclosure documented 3,056,950 affected individuals.

Deduplication of multi-state filings is the central operational challenge of multi-source compilation. The same incident is frequently filed with multiple state attorney general offices in addition to HHS OCR. The dashboard deduplicates by normalized entity name (lowercase, punctuation stripped, whitespace collapsed): records sharing a normalized entity name are treated as filings of the same incident, and the record with the highest reported affected-population value is retained on the working assumption that later state-level filings contain post-review revised totals. The Q1 2026 raw dataset of 218 records collapsed to 211 unique breach records via 7 multi-state pair collapses (TriZetto Provider Solutions, QualDerm Partners, Vikor Scientific, Expert MRI, Blue Shield of California, BlueCross BlueShield of Tennessee, Couve Healthcare Consulting). Following deduplication, four additional records were excluded from the final analytical set on healthcare-sector scope grounds (entities

operating outside healthcare and not serving as healthcare business associates), yielding the final deduplicated and scoped Q1 2026 dataset of 207 unique large healthcare breaches. The deduplication logic, the scope-filtering decisions, the audit trail, and known limitations are documented in Appendix D.

Affected-population figures throughout this paper are reported at the most recent publicly available value at the time of dashboard ingestion. In several Q1 2026 cases the figures reflect significant upward revisions from initial OCR placeholders. Where multiple sources report different affected-population values for the same incident, the higher (post-review) value is retained on the working assumption that data reviews complete monotonically.

Distinct from incident-record retention, the paper applies the Transparency-Adjusted Risk Function (Perrin, 2025b) qualitatively rather than quantitatively to the Q1 2026 record. The four component indices (DMVI, AAF, HTI, R) are not re-measured for Q1 2026 in this issue. Where the paper characterizes TARF components directionally (§5), it relies on structural reasoning and convergence across independent indicators rather than primary measurement. The methodological posture is described in §5 and Appendix C.

Four limitations specific to the Q1 2026 dataset deserve direct acknowledgment. First, the dashboard's HHS OCR ingestion lags the OCR portal by an estimated 1–3 weeks; some February 2026 OCR records present in the OCR portal as of late March may not yet appear in the dashboard's late-April export, accounting for the dashboard's slightly lower February count (47 vs. OCR's 63 at late-March access). Appendix D documents this gap. Second, the dashboard's State AG ingestion is concentrated in jurisdictions with active and accessible breach notification regimes (notably Oregon and California), and breach records for incidents disclosed only in jurisdictions with less accessible breach notification systems may be undercounted. Third, the deduplication logic treats incidents as identical if they share a normalized entity name and an exact affected-population count; incidents that have different affected-population counts at the time of ingestion (because OCR has not yet been updated with revised totals) may appear as duplicates. Fourth, the dashboard's archetype classification (used in §4) is structural-attribute based rather than first-public-label based, and is stable across quarters for year-over-year comparison purposes.

Theoretically, the paper applies the Transparency-Adjusted Risk Function from Perrin (2025b), reproduced in Figure 3: TARF = (DMVI × AAF × R) / HTI. Readers unfamiliar with the framework are directed to the source paper.

3. Q1 2026 Empirical Findings

3.1 Breach Volume and the Multi-Source Lift

The HHS OCR breach portal is the regulatory baseline for healthcare breach reporting in the United States. For Q1 2026 it is also a partial source. The portal recorded 46 large breaches in January 2026 (a 13.2% decline from December 2025 and the lowest January incident count since 2020), 63 breaches in February 2026 (a 14.5% month-over-month increase and 12.5% above the five-year February average), and only two breach reports for March 2026 as of April 10, 2026 (HHS OCR Breach Portal, 2026; calHIPAA, 2026a, 2026b). The cumulative January–February affected-population total stood at 9,651,076 individuals at late-March 2026 portal access. The investigation-pending queue stood at 978 cases as of January 31, 2026.

The Patient Protect Breach Intelligence Dashboard, the multi-source compilation described in §2 and audited in Appendix D, records a materially fuller picture for the same period. After deduplication of multi-state filings and exclusion of records outside healthcare-sector scope, the dashboard contains 207 unique large healthcare breaches with reported dates in Q1 2026, distributed across 80 in January, 47 in February, and 80 in March, affecting approximately 15.9 million individuals (Patient Protect Breach Intelligence Dashboard, 2026). Two complementary lift comparisons frame the contribution. Against the late-March 2026 OCR-only snapshot of 118 breaches (January–February only, with only two March entries available at late-March access), the dashboard's 207-breach full-quarter view represents an empirical lift of approximately 75%; this is the comparison most relevant to a researcher attempting to characterize the period using OCR alone at the time the quarter closed. Against the late-April 2026 OCR-only deduplicated count of 169 records (after OCR backlog clearance for March), the dashboard's 207-breach view represents a 22% lift attributable to state attorney general filings the OCR portal has not yet captured. The first comparison is not strictly apples-to-apples because the access dates differ; the second is, and demonstrates that the multi-source advantage persists beyond the immediate post-shutdown reporting catch-up.

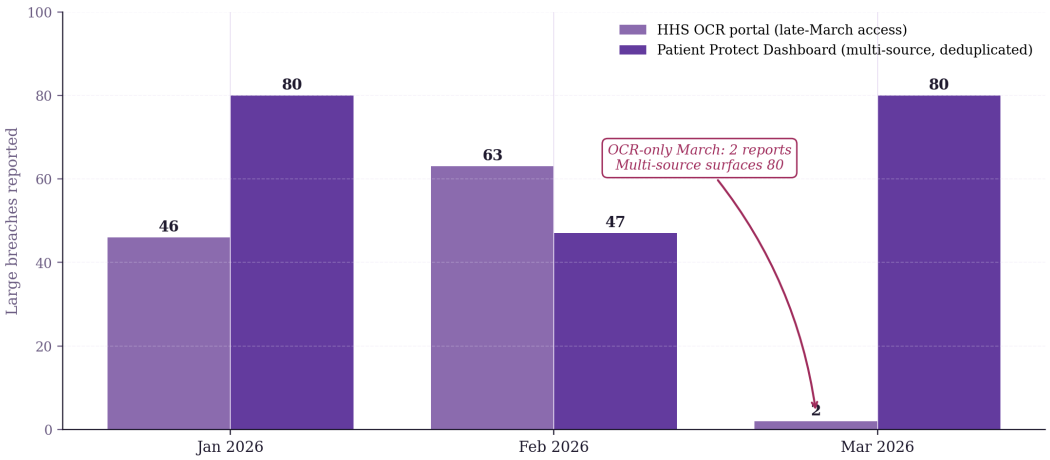
The lift is not noise. It is the predictable output of a reporting infrastructure in which OCR is one of many channels through which a healthcare breach becomes publicly known. State attorney general filings, particularly the Oregon AG's filings under the Oregon Consumer Information Protection Act, surfaced four of the period's largest incidents (TriZetto, QualDerm, Healthcare Interactive, Insightin Health) weeks to months before the corresponding HHS OCR portal entries appeared. CISA advisories, FTC enforcement actions, and primary entity disclosures captured the remaining lift. The 43-day federal government shutdown of late 2025 amplified the multi-source advantage by suspending OCR portal updates while state-level reporting continued.

Viewed against the trailing twelve-month baseline, OCR-only reporting sits within a reduced-reporting regime that began in the latter half of 2025. For the five-month period from April through August 2025, OCR received an average of 68.6 large breach reports per month. For the subsequent five-month period from September 2025 through January 2026, the average fell to 46.2 breaches, a 32.7% decline (Figure 2). The decline coincides temporally with the federal shutdown and is not cleanly attributable to any non-reporting factor in the OCR-only data. The dashboard's multi-source view of the same period shows breach activity continuing through the shutdown via state-level reporting, indicating that the OCR-only decline is at least partially a reporting artifact rather than an underlying threat-environment shift.

The full Q1 2026 picture used throughout the remainder of this paper is the deduplicated and healthcare-sector-scoped multi-source dashboard total of 207 breaches and approximately 15.9 million affected

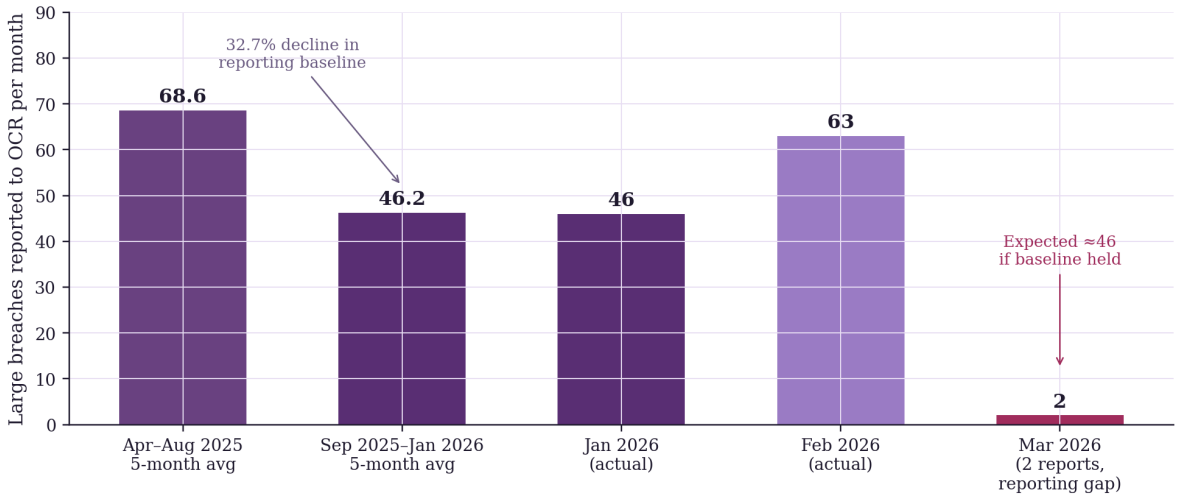
individuals. Where claims rest on OCR-only data (for example, year-over-year breach-count comparisons against historical OCR baselines), the source is explicitly identified.

Figure 1. Q1 2026 Healthcare Breach Volume — OCR-Only vs Multi-Source Compilation



Sources: HHS OCR Breach Portal (2026, late-March access); Patient Protect Breach Intelligence Dashboard (2026, late-April access). Dashboard figures deduplicated across multi-state filings.

Figure 2. OCR Large-Breach Reporting — Verified Data Points Only



Sources: HHS OCR Breach Portal (2026); calHIPAA (2026a, 2026b). No monthly values are interpolated.

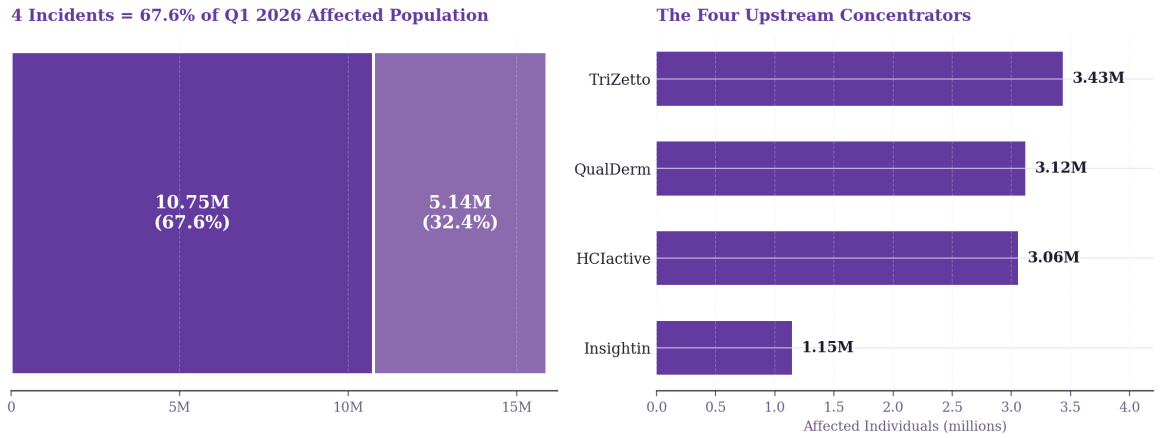
Sources: HHS OCR Breach Portal (2026); calHIPAA (2026a, 2026b). Figure shows verified data points only: the two 5-month reporting averages derived from OCR breach portal records, the two verified monthly totals for Jan and Feb 2026, and the late-March OCR portal access state for March 2026. The dashboard's full multi-source view of the same period is shown in Figure 1.

3.2 Concentration: Four Incidents, 67.6% of Population Impact

The most consequential finding of the Q1 2026 dataset is concentration. Four upstream business associate and platform-vendor incidents, together representing 1.9% of the period's deduplicated incident count, account for 67.6% of all affected individuals in the multi-source dataset (Figure 7). The four incidents are TriZetto Provider Solutions (3,433,965 affected; Oregon AG filing February 11, 2026; HHS OCR portal entry March 3, 2026), QualDerm Partners (3,117,874 affected; Oregon AG filing February 23, 2026; HHS OCR portal entry March 23, 2026), Healthcare Interactive / HCIactive (3,056,950 affected; OCR placeholder filing September 22, 2025; Oregon AG full disclosure January 7, 2026), and Insightin Health (1,144,686 affected; California AG filing

March 4, 2026; multi-state filings January–March 2026). Together they account for 10,753,475 of the approximately 15.9 million Q1 2026 affected individuals.

Figure 7. Q1 2026 Concentration: 1.9% of Incidents, 67.6% of Population Impact



Sources: Patient Protect Breach Intelligence Dashboard (2026); Oregon Attorney General; California Attorney General; HHS OCR Breach Portal (2026). N=207 unique Q1 2026 healthcare breaches.

The four upstream concentrators together account for 67.6% of Q1 2026 affected individuals across 1.9% of the period's deduplicated incident count. Sources: Patient Protect Breach Intelligence Dashboard (2026); Oregon Attorney General; California Attorney General; HHS OCR Breach Portal (2026).

The concentration is not an artifact of dataset construction. It reflects the underlying market structure of healthcare data processing, in which a small number of upstream platform vendors and business associates aggregate PHI across hundreds of covered entities. A single intrusion at TriZetto, which provides administrative services to insurers and providers as a subcontractor to OCHIN and other entities, propagates downstream into hundreds of separate covered-entity breach notifications. A single intrusion at Healthcare Interactive (HCIactive), which provides AI-powered insurance enrollment and benefits administration to multiple health plans, surfaced 103,000 affected individuals in South Carolina alone, with the full scope reaching 3,056,950 across at least eight states. A single intrusion at Insightin Health, exploiting a zero-day in the GoAnywhere file-transfer tool and claimed by the MEDUSA ransomware group, surfaced affected populations across California, Oregon, Texas, Vermont, Washington, and Rhode Island.

The structural finding sharpens the upstream concentration thesis identified in Perrin (2025a). The 67.6% concentration ratio is the empirical evidence that healthcare cybersecurity risk is not uniformly distributed across covered entities; it is mechanically concentrated at upstream nodes whose security posture, breach response capability, and disclosure speed determine the sector's aggregate risk profile. Q1 2026 also illustrates the propagation lag inherent in the cascade. Each of the four upstream incidents will continue to populate downstream covered-entity breach notifications across Q2 2026 and later quarters as covered entities work through their own notification obligations, meaning aggregate breach counts in subsequent OCR reporting will systematically over-count incident frequency relative to root-cause incident frequency.

OCR-only reporting for January and February 2026 showed 9,651,076 affected individuals across the 118 January–February incidents. The dashboard's full Q1 multi-source total of approximately 15.9 million reflects (a) the addition of 80 March 2026 breaches not yet visible in the OCR-only late-March snapshot, (b) revised affected-population totals for incidents whose initial OCR placeholders were updated through state-level filings (notably Healthcare Interactive's revision from 501 placeholder to 3,056,950 confirmed), (c) state attorney

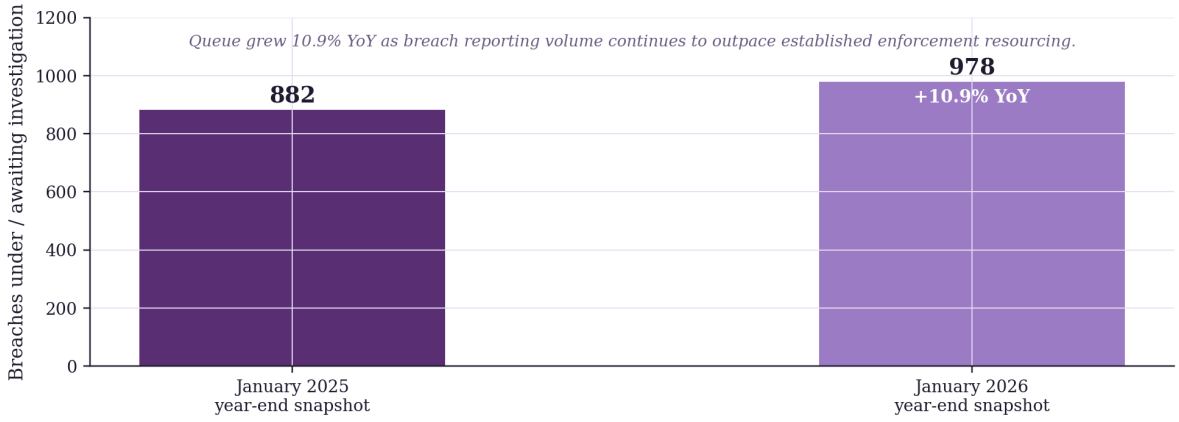
general filings for incidents that had not yet appeared in the OCR portal, and (d) exclusion of four records outside healthcare-sector scope (4,658 affected individuals removed). The reconciliation between the OCR-only and multi-source views is detailed in Appendix B; the scope-filter rationale is described in Appendix D.

> **KEY FINDING — §3.2**
>
> Four upstream incidents (TriZetto, QualDerm, HCIactive, Insightin Health) together drove 10.75M of the approximately 15.9M Q1 2026 affected individuals — 67.6% of the period's population impact across 1.9% of its incident count. The concentration is the empirical signature of upstream business associate aggregation, not a sampling artifact.

3.3 The OCR Investigation Queue as a Leading Indicator

The OCR breach investigation queue warrants its own analytical treatment. As of January 31, 2026, 978 healthcare data breaches were under or awaiting investigation by OCR, based on the OCR breach portal snapshot (HHS OCR Breach Portal, 2026; calHIPAA, 2026a). This figure rose from 882 at the comparable date in January 2025, a 10.9% year-over-year increase (Figure 6). The growth occurred during a period in which breach reporting volume has approximately doubled since 2018 while OCR's resourcing has remained largely stable; this dynamic is documented in independent industry reporting and is consistent with the broader pattern of healthcare cybersecurity workload outpacing federal civil rights enforcement capacity across administrations (TechTarget/HealthITSecurity, 2025; Paubox, 2025). The queue's growth predates the late-2025 shutdown and reflects a structural workload-to-resourcing dynamic rather than an episode-specific issue.

Figure 6. OCR Breach Investigation Queue — Verified Year-End Snapshots



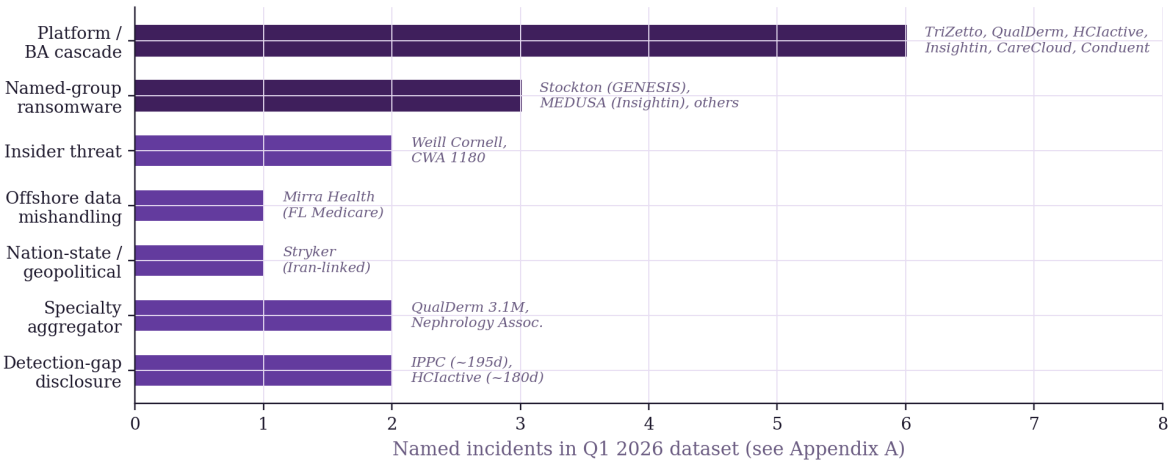
Sources: HHS OCR Breach Portal (2026); calHIPAA (2026a); Paubox (2025); TechTarget/HealthITSecurity (2025).

The policy implication is structural. If the ratio of incidents to resolutions continues to widen, the timing profile of post-incident OCR enforcement, historically one component of the broader compliance environment alongside civil litigation risk, will shift toward longer post-incident intervals. The current OCR strategy of prioritizing risk-analysis cases (45 CFR §164.308(a)(1)(ii)(A)) is a sensible adaptation to the prevailing workload mix: risk-analysis cases can be resolved on shorter timelines than full breach investigations, allowing OCR to maintain enforcement signal across a larger portfolio of cases.

4. Anatomy of Q1: Seven Attack Archetypes

A quarterly breach review that reports only aggregate counts misses the diagnostic value of the incident record. The Q1 2026 period produced a set of named incidents that are not interchangeable. Each represents a distinct structural pathway — a different combination of attack surface, threat actor motivation, data concentration, and detection failure. The seven archetypes that follow are not exhaustive of Q1 activity, but together they characterize the period.

Figure 4. Attack Archetype Distribution — Named Q1 2026 Cases



4.1 Platform and Business-Associate Cascade

TriZetto · QualDerm Partners · Healthcare Interactive (HCIactive) · Insightin Health · CareCloud · Conduent (2025 origin)

The platform and business-associate cascade is the dominant archetype of Q1 2026 by population impact. Four upstream incidents drove 67.6% of the period's affected individuals.

TriZetto Provider Solutions, a healthcare payments and claims processing business associate that operates as a subcontractor to OCHIN and other healthcare technology vendors, disclosed a 2025-origin breach affecting 3,433,965 individuals; the Oregon AG was notified February 11, 2026, and the HHS OCR portal entry followed March 3, 2026 (HHS OCR Breach Portal, 2026; Oregon Attorney General, 2026; Fox News, 2026). OCHIN reported that the incident affected approximately 9% of its member network, or approximately 700,000 patients (Bank Info Security, 2025).

QualDerm Partners, a dermatology practice aggregator providing management services to 158 healthcare practices in 17 states, disclosed a Q1 2026 incident affecting 3,117,874 individuals; the intrusion was confirmed between December 23 and December 24, 2025 (HHS OCR Breach Portal, 2026; Oregon Attorney General, 2026).

Healthcare Interactive (HCIactive), an Ellicott City, Maryland-based provider of AI-powered insurance enrollment and benefits administration software, disclosed an incident affecting 3,056,950 individuals; the unauthorized access window was identified as July 8–12, 2025, with the Oregon AG suggesting a potentially

longer window of June 17 to July 22, 2025 (HCIactive, 2026; Paubox, 2026; Oregon Attorney General, 2026; This Week Health, 2026). The incident illustrates the placeholder-revision dynamic central to multi-source compilation: HCIactive filed an OCR placeholder of 501 affected individuals on September 22, 2025, while review remained open; the Oregon AG was notified of the full 3,056,950 figure on January 7, 2026, more than three months before the OCR portal reflected the revised total.

Insightin Health, a Baltimore-based AI-powered platform for health insurer and payer data analytics, disclosed an incident affecting 1,144,686 individuals after exploitation of a previously unknown vulnerability in the GoAnywhere file-transfer tool between September 17 and September 23, 2025 (Insightin Health, 2026; Comparitech, 2026; California Attorney General, 2026). The MEDUSA ransomware group claimed responsibility on September 26, 2025, asserting exfiltration of 378 GB of data; Insightin Health has not publicly acknowledged the MEDUSA claim. State filings spanned California, Oregon, Texas, Vermont, Washington, and Rhode Island (DataBreaches.net, 2026).

CareCloud, an electronic health record platform serving more than 45,000 U.S. medical providers, was reported in late March 2026 to have experienced unauthorized access to an EHR environment containing patient data; the incident is referenced here based on public secondary reporting and the dashboard's modeled-threat-signal channel rather than a primary HIPAA breach filing, and is excluded from the deduplicated 207-incident analytical dataset pending primary-source confirmation (Zeron, 2026). Conduent Business Solutions, the subject of a February 2025 SafePay ransomware group claim asserting 8.5 terabytes of exfiltration (Bank Info Security, 2025), continued to produce downstream covered-entity notifications across the Q1 2026 period.

Aggregate breach counts systematically under-represent the impact of upstream incidents because each downstream covered-entity notification is counted as an incident of its own, even when one upstream business associate is the actual root cause. The 1.9% / 67.6% concentration ratio (4 incidents driving 67.6% of population impact) is the empirical demonstration of the asymmetry. Subsequent quarters will see the four incidents continue to populate downstream covered-entity breach notifications as covered entities work through their own notification obligations.

4.2 Named-Group Ransomware

Stockton Cardiology (GENESIS) · QualDerm Partners

The Stockton Cardiology Medical Group incident illustrates the fully-documented timeline of a named-group ransomware case. The initial phishing compromise occurred on December 15, 2025, when suspicious emails were sent to practice employees and subsequently deleted (Paubox, 2026; The Lyon Firm, 2026). Internal discovery of unauthorized file access followed on January 17, 2026 — a 33-day detection gap. Public disclosure occurred on February 17, 2026, when the GENESIS ransomware group claimed responsibility via dark-web leak-site post, asserting the exfiltration of 645 gigabytes of personal, healthcare, financial, and operational data (Paubox, 2026; RedPacket Security, 2026; Becker's ASC Review, 2026). Formal reporting to the California Attorney General followed on March 20, 2026 (The Lyon Firm, 2026). The attack-to-public-leak gap was 64 days; the attack-to-formal-notification gap was 95 days. Stockton's formal notification process was initiated in response to the leak-site publication, not in advance of it — an inversion of the disclosure sequence that HIPAA contemplates.

QualDerm Partners, a dermatology practice aggregator, reported a Q1 2026 incident affecting 3.1 million individuals. The specialty-aggregator subtype represents a growing subcategory within the ransomware archetype: consolidated specialty practices with shared IT infrastructure present a large affected-population surface with a relatively compact attack surface.

Named-group attribution itself has become an operational norm. GENESIS, SafePay, and additional groups featured in Q1 leak-site activity against healthcare targets. The leak-site publication pathway is now a common vector for public disclosure, frequently preceding formal regulatory notification.

4.3 Insider Threat

Weill Cornell Medicine · CWA Local 1180

Weill Cornell Medicine disclosed a data breach in Q1 2026 characterized in public reporting as insider-origin. Insider incidents are diagnostically important because they are not addressable by perimeter security, encryption, or endpoint detection alone. They require access control review, role-based permission hygiene, audit log retention, and behavioral analytics — controls that are present in the HIPAA Security Rule but unevenly implemented. The Q1 insider incidents underscore that technical controls alone are insufficient and that the administrative safeguards of the Security Rule (45 CFR §164.308) carry operational weight commensurate with the technical safeguards of §164.312.

4.4 Offshore Data Mishandling

Mirra Health (Florida Medicare)

Mirra Health was publicly reported in late March 2026 to have exposed the data of Florida Medicare members after improperly outsourcing records overseas. As with the CareCloud reference in §4.1, the Mirra reference here is sourced through the dashboard's modeled-threat-signal channel and public secondary reporting rather than a primary HIPAA breach filing; it is referenced for archetype illustration and is excluded from the deduplicated 207-incident analytical dataset pending primary-source confirmation. The archetype itself is structurally important regardless of the specific case attribution: it does not require a hacker; it requires only a business-associate agreement implementation gap. Under the HIPAA Privacy Rule, offshore data processing is not prohibited, but it must be governed by a compliant BAA that extends HIPAA-equivalent protections to the processing entity. Where these gaps occur, they illustrate a sub-pattern visible elsewhere in the Q1 record: the regulatory burden of offshore data handling is increasingly disproportionate to its labor-cost advantage, particularly when combined with state-level consumer privacy enforcement and the reputational consequences of public disclosure.

4.5 Nation-State / Geopolitical

Stryker (Iran-linked attribution)

Stryker — a medical device manufacturer — was publicly reported in late March 2026 to have contained a cyberattack that has been linked in open-source reporting to Iran-affiliated actors. The Stryker reference here is sourced through the dashboard's modeled-threat-signal channel and public secondary reporting rather than a primary HIPAA breach filing, and is excluded from the deduplicated 207-incident analytical dataset; it is included in this archetype discussion because the reporting boundary it illustrates is itself a structural finding worth surfacing. Two attribution caveats apply. First, nation-state attribution in cyber incidents is inherently probabilistic rather than definitive, and readers should treat the open-source linkage as a working characterization rather than a finding of fact. Second, medical device cyberattacks may not trigger HIPAA breach reporting obligations in the same way conventional PHI breaches do; this is in part why the incident appears via modeled-threat-signal rather than via the OCR portal. With those caveats noted: a publicly-reported nation-state targeting of a U.S. medical device manufacturer is categorically distinct from the more common

ransomware and business-associate archetypes that dominate the Q1 record. Medical device cybersecurity is regulated primarily through FDA premarket and postmarket guidance, not through OCR enforcement, and the coordination gap between the two regulatory regimes is a known structural feature. The Stryker incident sits most clearly outside the HIPAA enforcement perimeter — and its absence from primary HIPAA filings, even in an apparent breach scenario, is itself diagnostic.

4.6 Detection-Gap Disclosure

Innovative Pharmacy Packaging Corp · late-disclosure long-tail

Innovative Pharmacy Packaging Corp (IPPC), a New Jersey long-term care pharmacy, reported that unauthorized network access had occurred between September 18 and September 19, 2025. Review of the affected files concluded on February 9, 2026 (Mass.gov, 2026; ClaimDepot, 2026). IPPC posted a notice on its website on February 27, 2026, approximately 162 days after the initial compromise. Individual notification letters were dated April 1, 2026 — approximately 195 days after the initial compromise (Mass.gov, 2026; Cole & Van Note, 2026; Paubox, 2026b). The HHS OCR portal entry for IPPC was filed April 8, 2026 with 133,862 affected individuals, placing the OCR record itself outside the Q1 2026 reporting window. IPPC is included in this archetype discussion because its disclosure timeline straddles the Q1 boundary — the substitute breach notice was published in late February 2026 — and because the 195-day detection-to-notification gap is the single most diagnostic Q1 example of the long-latency archetype. The incident is excluded from the deduplicated 207-incident Q1 dataset on reportedDate grounds and will be included in the Q2 2026 issue's empirical record.

IPPC is not the only late disclosure of a 2025-origin incident referenced in this paper; the period record contains multiple instances of multi-month detection-to-disclosure gaps. The disclosure-gap archetype is the most direct empirical refutation of the hypothesis that declining reported breach counts reflect declining breach activity. The IPPC, TriZetto, Healthcare Interactive, Insightin Health, and Conduent cascades all originate in 2025 with disclosure events landing in Q1 2026 or just outside it.

4.7 Telehealth-Sector Targeting

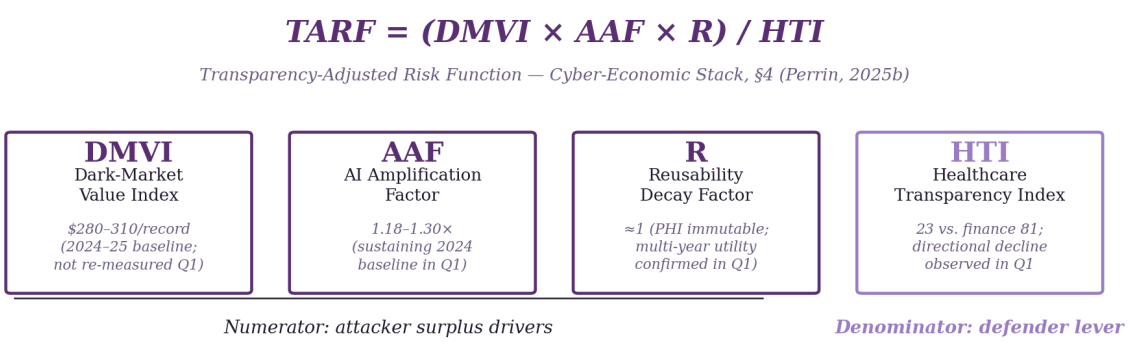
Two telehealth incidents — 3.7M patients combined

Two separate telehealth breaches reported in late March 2026 collectively affected an estimated 3.7 million patients. Telehealth platforms sit structurally between traditional covered entity infrastructure and consumer-facing digital health, and they carry an attack surface that has grown materially since 2020. The Q1 telehealth incidents concentrated affected-population impact in a small number of breaches, consistent with the platform-cascade dynamic described in §4.1.

5. Structural Analysis: The TARF Framework Applied

The empirical record of Q1 2026 is not a random walk. It is the predictable output of the structural conditions described in prior Secure Care Research Institute working papers. In this section we apply the Transparency-Adjusted Risk Function (Perrin, 2025b) to the Q1 context. The application is qualitative rather than quantitative: the four component indices are not re-measured for Q1 2026 in this issue, and a full numerical recomputation is a candidate for a dedicated future paper. Where quantitative re-measurement is not performed, directional conclusions in this paper are based on convergence across independent indicators rather than single-source inference. What follows is a structural characterization of each component against the observed Q1 record.

Figure 3. The TARF Framework — Qualitative Application to Q1 2026



Q1 2026 qualitative finding: Numerator stable-to-rising; HTI directionally deteriorated

Detection-to-disclosure gaps in named Q1 cases ranged from ~64 days (Stockton leak) to ~195 days (IPPC individual notification).

5.1 DMVI — Dark-Market Value Index

The Dark-Market Value Index for full-package PHI records was established in prior Secure Care Research Institute work at $280–310 per record, based on 2024–2025 dark-market observations from multiple threat intelligence sources (Perrin, 2025b; citing Intel 471, Recorded Future, and Flashpoint, 2024–2025). This paper does not re-measure DMVI for Q1 2026, and dark-web pricing is characteristically volatile and opaque; the $280–310 figure should therefore be read as a 2024–2025 baseline rather than a Q1 2026 measurement.

Multiple independent sources published during 2025 corroborate the order-of-magnitude claim that PHI retains a substantial pricing premium over other stolen data types, even as specific price points vary. The HHS HC3 Intelligence Briefing on the Dark Web PHI Marketplace reports an average value of approximately $250 per record with a ceiling near $1,000 (cited in Applied Tech, 2025). IBM X-Force (2025) reports healthcare records selling for approximately $250 each in dark web shops. Total Assure's 2025 cybersecurity statistics report a ceiling as high as $1,200 per record for complete PHI packages. These independent observations are consistent with the SCRI baseline band and also consistent with the structural claim — PHI's immutability and multi-domain fraud utility sustain a premium over credit card data — but they should not be read as Q1 2026–specific measurements.

The structural factors supporting the pricing premium over stolen credit card data — immutability of PHI records, multi-domain fraud utility, multi-year retention of value — remained in place across the Q1 window. No public signal of commoditization, supply glut, or successful law enforcement market disruption was observed during Q1 2026 that would indicate structural downward pressure on PHI pricing. The working assumption for the remainder of this analysis is therefore that the 2024–2025 DMVI baseline remains *directionally* applicable as a modeled input to the TARF framework. A Q2 2026 revisit with primary dark-market observations is appropriate.

5.2 AAF — AI Amplification Factor

The AI Amplification Factor identified in the Cyber-Economic Stack paper (1.18–1.30 post-ChatGPT) modeled the multiplier effect of generative AI on per-record fraud yield (Perrin, 2025b). A direct quantitative re-measurement for Q1 2026 is not performed in this issue, and this paper does not claim direct attribution of any Q1 2026 breach to a generative-AI-enabled primary attack vector.

Independent 2025 evidence is consistent with continued AI-enabled fraud expansion in healthcare. The Department of Justice's 2025 National Healthcare Fraud Takedown charged 324 defendants with $14.6 billion in alleged intended loss, with AI-generated consent fraud explicitly identified as a featured scheme category (Medical Economics, 2026). The DOJ and HHS jointly flagged manipulation of electronic health record systems, including prompts generated by AI algorithms, as a priority enforcement area (Keller Grover, 2026). TruthScan's 2025 whitepaper documents AI-generated medical documents, forged prescriptions, deepfaked doctor-patient interactions, and AI voice scams targeting older adults as 2025 healthcare fraud categories (TruthScan, 2025). Pindrop Security (2025) reports a 475% year-over-year increase in voice-cloning fraud directed at healthcare insurers in 2024.

These observations support the directional claim that AI amplification of healthcare fraud continued through 2025 and into 2026. They do not, however, establish a specific Q1 2026 AAF value, and none of the named Q1 2026 breaches in Appendix A has been publicly attributed to an AI-enabled primary attack vector. The AAF is treated in this paper as a modeled input consistent with prevailing evidence, not as a Q1-measured quantity.

5.3 R — Reusability

PHI reusability in the Q1 record approaches unity. Social Security numbers, birth dates, and diagnostic codes exposed in Q1 incidents will retain fraud utility for years; insurance policy identifiers and Medicare IDs can be used in claim fraud across multiple fiscal periods. The IPPC incident's approximately 195-day detection-to-notification gap illustrates this directly: exfiltrated data from a September 2025 incident retained sufficient market value through April 2026 individual notification that affected patients remained at elevated fraud risk during the entire intervening period, without notification and without the ability to take protective action.

5.4 HTI — Healthcare Transparency Index

The denominator of the TARF equation is where Q1 2026 is most diagnostic. The Healthcare Transparency Index compares disclosure speed, richness, and cadence across sectors. Healthcare scored 23 against finance's 81 in prior research (Perrin, 2025b); the gap reflects the substantially different regulatory architectures of the two sectors (HIPAA's 60-day disclosure window versus SEC Item 1.05 Form 8-K's 4-business-day requirement) more than it reflects any judgment about either regulator's performance. A quantitative HTI recalculation for Q1 2026 is outside the scope of this issue. Directionally, however, the Q1 2026 record is consistent with the prior gap rather than evidence of convergence: the OCR portal queue grew 10.9% year-over-year to 978 open cases,

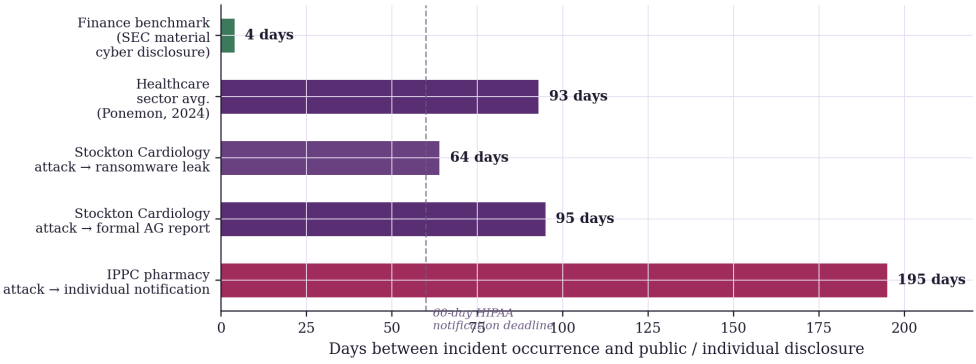
March 2026 OCR reporting reflected the late-2025 shutdown's lingering effects, named-incident detection-to-disclosure intervals in the quarter ranged from approximately 64 days (Stockton Cardiology, attack → ransomware leak publication) to approximately 195 days (IPPC, attack → individual notification), and the Stockton Cardiology public disclosure path was driven by the ransomware group's leak-site posting before the covered entity's formal notification — an inversion of the typical HIPAA disclosure sequence that is illustrative of the pressures the current regime operates under. A formal HTI reassessment is a candidate for a future dedicated working paper.

Because HTI appears in the TARF denominator, any directional decline inflates the transparency-adjusted risk function for every covered entity and business associate in the sector, independent of any change in DMVI, AAF, or R. This is the most important structural observation of the period.

5.5 The TARF Equation in Q1 2026

Synthesizing the four components qualitatively: the Q1 record shows a stable-to-modestly-rising numerator (DMVI at prior baseline; AAF sustaining the 2024 multiplier; R at near-unity given the multi-month latency of disclosures in the Q1 case set) against a denominator under continued workload pressure (HTI continuing to reflect the structural sector gap, with reporting cadence and detection-to-disclosure intervals consistent with a queue operating near capacity). Per the TARF framework, that configuration is directionally consistent with sustained sector-wide exploitability in Q1 2026 even as reported incident counts declined. The framework treats the denominator as a function of the broader healthcare reporting and enforcement environment, in which OCR is one node alongside state attorneys general, the FTC, CISA, and the regulated entities themselves. A numerical recomputation of the function for Q1 2026 is not undertaken in this issue; the directional reading should be read as a hypothesis-generating output of the framework, not an empirical demonstration.

Figure 5. Detection-to-Disclosure Latency — Sector Benchmarks and Named Q1 2026 Cases



Sources: Paubox (2026a, 2026b); The Lyon Firm (2026); Becker's ASC Review (2026); Mass.gov (2026); Perrin (2025b) citing Ponemon (2024); SEC Form 8-K Item 1.05.

Detection-to-disclosure latency in named Q1 2026 cases vs. sector benchmarks. Finance benchmark is the SEC 4-business-day rule for material cybersecurity incidents.

6. The Regulatory Inflection: What Q1 Reveals About 2026

Q1 2026 carried three regulatory developments — and one overarching regulatory uncertainty — that together position 2026 as a potential inflection year for the HIPAA regulatory architecture. The pending updates would represent the most significant changes to the Security Rule in more than a decade if finalized as proposed.

6.1 Part 2 Integration (February 16, 2026)

Effective February 16, 2026, OCR's civil enforcement authority over 42 CFR Part 2 substance use disorder records took effect, and OCR began accepting Part 2 breach notifications and complaints of alleged Part 2 violations through a dedicated form on its existing breach reporting portal (TechTarget/HealthITSecurity, 2026; Alston & Bird, 2026). The change represented the first time Part 2 breach notifications were processed through the same public-facing reporting channel as HIPAA breaches, closing a longstanding gap in which Part 2 records, among the most sensitive in healthcare, were reported through a separate and less transparent channel. Covered entities and business associates handling SUD data now face a unified breach reporting obligation and a unified public-record exposure model. The Top of the World Ranch Treatment Center OCR settlement three days later, on February 19, 2026, may be read in part as an enforcement signal accompanying the expansion.

6.2 Enforcement Signals: Risk Analysis Remains the Primary Lever

The Top of the World Ranch Treatment Center settlement — $103,000 resolving alleged noncompliance with 45 CFR §164.308(a)(1)(ii)(A), the risk analysis requirement — is the clearest enforcement signal from the Q1 2026 period (Hunton Andrews Kurth, 2026). The underlying incident was a March 2023 phishing attack; the settlement was February 19, 2026. The enforcement principle, however, is that a documented and ongoing risk analysis is the single most durable compliance lever, and that its absence is sanctioned independently of the downstream breach. Independent industry reporting confirms OCR's ongoing risk-analysis enforcement initiative, initially announced in 2024, continues as a strategic priority in 2026 and has been expanded to also cover risk management; this strategy enables OCR to resolve a material share of its hacking-incident investigations more efficiently while focusing on the most commonly identified HIPAA Security Rule violation (TechTarget/HealthITSecurity, 2026; Paubox, 2026c).

A covered entity or business associate with no documented risk analysis, no current risk analysis, or a risk analysis that does not cover all ePHI-holding information systems is exposed to OCR enforcement regardless of whether a breach occurs. The Q1 enforcement signal is that this exposure is being actively maintained, not narrowed.

6.3 The 2026 HIPAA Security Rule Update

The anticipated update to the HIPAA Security Rule is the single largest pending regulatory variable of 2026. On December 27, 2024, the HHS Office for Civil Rights issued a Notice of Proposed Rulemaking (NPRM) to amend the Security Rule (HHS Office for Civil Rights, 2024). The NPRM was published in the Federal Register on January 6, 2025, and the 60-day public comment period closed March 7, 2025. HHS received more than 4,000 public comments during that period (Paul Hastings, 2025; Medcurity, 2026).

The direction of the proposed changes is consistent and significant. Key provisions in the NPRM (HHS fact sheet, 2024; Paul Hastings, 2025; BDO, 2025) include: removal of the "addressable" versus "required" distinction for implementation specifications, making all safeguards mandatory with limited specified

exceptions; mandated encryption of ePHI at rest and in transit; mandatory multi-factor authentication, with exceptions for legacy systems and FDA-approved medical devices; vulnerability scanning at least every six months; penetration testing at least annually; timely access notifications within 24 hours of workforce access changes; and formalized documentation obligations. Assuming the NPRM's structure is largely preserved in the final rule, entities subject to the Security Rule (including those bound indirectly through business associate agreements) should anticipate a material compliance uplift.

The practical implication for covered entities and business associates is that the compliance program adequate in 2025 is unlikely to be adequate under the final rule. The mandatory encryption and MFA provisions alone will reclassify as violations a non-trivial fraction of currently-deployed environments. Practices that begin implementation in Q2 2026 will have a wider remediation window than those that wait for final rule publication.

6.4 Regulatory Freeze and Finalization Uncertainty

The 2026 HIPAA Security Rule update's finalization timeline is subject to material uncertainty. A January 20, 2025 executive order placed a regulatory freeze on pending rules pending administrative review (Johnson Lambert, 2025). Commentary from legal and compliance advisors has accordingly diverged on the likely final-rule publication timeline, with some sources anticipating May 2026 publication (Lexology, 2026; Medcurity, 2026) and others treating finalization as uncertain. The NPRM provides that the final rule's effective date would be 60 days after publication, with a compliance date 180 days after the effective date.

The practical posture recommended by multiple advisors — and consistent with the analytical framework of this paper — is that covered entities and business associates should treat the NPRM provisions as the probable future compliance baseline and begin implementation in advance of final rule publication, rather than await resolution of the freeze. The risk of over-preparing is modest (the controls in the NPRM are independently supported by prevailing cybersecurity best practices); the risk of under-preparing, if the rule is finalized with a short implementation window, is material.

7. Recommendations

The following recommendations are derived from the Q1 2026 empirical record and the analytical framework applied in §5. They are structured by audience. They do not constitute legal advice. Covered entities and business associates with specific compliance questions should consult qualified HIPAA counsel.

7.1 For Covered Entities

1. Complete or refresh the risk analysis.

The Top of the World Ranch settlement is the single clearest enforcement signal of the period. A current, comprehensive, documented risk analysis covering all ePHI-holding information systems is the primary compliance artifact OCR reviews after any incident. If the most recent risk analysis is older than twelve months or does not reflect current systems, it should be refreshed immediately.

2. Inventory business associates and verify BAA completeness.

Four of the seven Q1 attack archetypes traced to business associate or platform-level incidents. Every BA relationship should have a current, signed, complete business associate agreement; for any BA handling ePHI offshore, the BAA should include specific language regarding jurisdiction, access controls, and subcontractor oversight.

3. Prepare for mandatory encryption and MFA.

The 2026 Security Rule update NPRM elevates encryption and multi-factor authentication from 'addressable' to 'required' (with limited exceptions). Covered entities should inventory unencrypted ePHI stores and systems lacking MFA now, before final rule publication. The cost of pre-positioning is lower than the cost of retroactive remediation under a short compliance window.

4. Shorten the internal detection-to-disclosure loop.

The sector-average 93-day detection gap (Ponemon, 2024) is cumulative across every subsequent harm. Even absent regulatory change, covered entities benefit from internal targets — for example, a 30-day internal target from detection to OCR notification — that are tighter than the 60-day regulatory maximum. Internal targets should be documented in breach response procedures.

5. Assume upstream incidents will propagate.

Given the Q1 platform and business-associate cascade archetype, covered entities should treat the CareCloud, TriZetto, Conduent, and telehealth-platform disclosures as advance notice of pending downstream notification obligations. Breach response procedures should be rehearsed for the scenario in which a BA disclosure triggers a covered entity notification obligation with short lead time.

7.2 For Business Associates

1. Accept that business-associate risk is the period's dominant story.

The structural concentration of PHI at business associates and platform vendors means the highest-impact Q1 incidents originated upstream of covered entities. Business associates should recognize this shift in the threat distribution and reciprocally harden their own security posture to a standard that exceeds the current covered-entity baseline.

2. Maintain current risk analyses and vulnerability assessments.

The risk analysis obligation under 45 CFR §164.308(a)(1)(ii)(A) applies to business associates. The Top of the World Ranch enforcement logic applies with equal force to any business associate that has not completed a current risk analysis.

3. Publish a security posture summary accessible to covered-entity customers.

The Healthcare Transparency Index deficit identified in §5.4 is partially addressable at the business associate level. Publishing a current security posture summary — including encryption standards, MFA posture, penetration test cadence, BAA terms, and breach notification timelines — closes part of the asymmetry that covered-entity customers face when assessing upstream risk.

4. Prepare for expanded BA oversight provisions.

The 2026 Security Rule update is expected to expand business associate oversight requirements, including documented verification of subcontractor BAAs and tightened audit obligations. Business associates should not wait for final rule publication to inventory and document their subcontractor chain.

7.3 For Regulators and Policy Makers

1. Continued investment in OCR breach portal infrastructure capacity would compound public benefit.

The 978-breach investigation queue and the late-2025 shutdown-induced reporting pause illustrate the operational sensitivity of the breach reporting infrastructure to volume and funding continuity. The Healthcare Transparency Index is, in the TARF framework, a key component of the defender-side architecture. Its operational instantiation is the OCR breach portal alongside parallel state attorney general reporting channels. Portal capacity, update frequency, automated ingestion, and resilience to funding interruptions are material public goods, and continued investment in this infrastructure produces benefits that compound across the sector.

2. Phased shortening of mandatory disclosure timelines warrants policy evaluation.

The finance sector's 4-business-day SEC Item 1.05 Form 8-K requirement provides one cross-sector benchmark, though direct comparison should be qualified by the substantially different regulatory architectures and data sensitivity profiles of the two sectors. Modeling in Perrin (2025b) projects that halving healthcare's 93-day detection-to-disclosure window could reduce sector-wide exploit ROI by an estimated 25–35%, which, applied to the Cyber-Economic Stack's fraud base, yields a modeled suppression estimate in the $8 to $12 billion annual range. This figure is a modeled output rather than an observed savings number; it depends on prior-paper assumptions not re-derived here. It is consistent in scale with independent 2025 evidence (DOJ's 2025 National Healthcare Fraud Takedown alleged $14.6B in intended loss; industry estimates place total annual healthcare fraud losses in the $68B-and-higher range). A phased evaluation of a tighter HIPAA notification window for large incidents — perhaps a 30-day target above a defined affected-population threshold — warrants policy consideration, balanced against the operational realities of active incident response.

3. Strengthened cross-agency coordination on medical-device cybersecurity merits attention.

The Stryker incident sits at the operational seam between HIPAA enforcement (OCR) and medical device cybersecurity oversight (FDA), with relevant equities also held by CISA and CMS. The publicly-attributed nation-state actor in this Q1 case indicates the seam is being actively probed. Formalized coordination mechanisms across these agencies — building on existing informal cooperation — would be a constructive structural improvement, recognizing that each agency operates within its own statutory authority.

4. Finalization of the 2026 HIPAA Security Rule update would be a substantial sector improvement.

The pending Security Rule update represents an opportunity to advance the sector's baseline technical posture (encryption, MFA, vulnerability scanning, penetration testing) in line with prevailing cybersecurity practice. The update process has appropriately accommodated the January 2025 regulatory freeze and the substantial public-comment volume. Finalization at the earliest practicable date, consistent with regulatory due process, would deliver compounding security and reporting-clarity benefits across the sector.

8. Conclusion

The Q1 2026 multi-source empirical record — 207 unique large healthcare breaches across January, February, and March, affecting approximately 15.9 million individuals — establishes a different picture than OCR-only reporting suggests. The OCR portal alone, accessed in late March 2026, recorded 118 January–February breaches and only two March reports, an OCR-only view that would have admitted an optimistic reading of a quietly improving threat environment. The full multi-source record does not support that reading.

The Q1 named-incident set reveals a concentrated attack archetype distribution in which four upstream business associate and platform-level incidents (TriZetto, QualDerm, Healthcare Interactive, Insightin Health) accounted for 67.6% of the period's affected individuals across just 1.9% of its incident count. The detection-to-disclosure intervals in named Q1 cases ranged from approximately 64 to 195 days; the comparable sector average is 93 days (Ponemon, 2024) and the SEC Item 1.05 Form 8-K finance-sector requirement is 4 business days. The cross-sector comparison reflects substantially different regulatory architectures and is not a judgment about the relative performance of either regulator. The OCR investigation queue grew to 978 incidents during the period, reflecting continued workload volume against established enforcement resourcing. A 43-day federal government shutdown affected OCR reporting cadence in late 2025 with continuing effects into Q1 2026. A publicly-reported nation-state incident (Stryker, sourced via modeled-threat-signal channel rather than primary HIPAA breach filing — see §4.5) entered the period's discussion for the first time in the current quarterly series. The regulatory environment opened two new variables (Part 2 civil enforcement effective February 16, 2026, and sustained risk-analysis enforcement) while the largest pending variable, the 2026 HIPAA Security Rule update, remains in process, with finalization timing subject to uncertainty following the January 2025 regulatory freeze.

Applied qualitatively to this record, the TARF framework yields a directional finding. The numerator of transparency-adjusted risk was stable to modestly-rising while the denominator continued to reflect the structural sector gap identified in prior research. The Q1 2026 record is directionally consistent with sustained sector-wide exploitability, independent of the change in reported incident counts. The paper does not claim this as empirical proof. It claims this as the framework-derived hypothesis the data invites. This conclusion reflects structural inference across multiple independent indicators rather than direct measurement of exploitability; readers should evaluate it on the quality of the inferential chain rather than on an expectation of empirical proof the current data infrastructure does not yet permit.

The inaugural volume of the State of Compliance series accordingly establishes, as its central Q1 finding, that healthcare breach risk is mechanically concentrated at upstream business associate and platform-vendor nodes whose security posture and disclosure timing materially shape the sector's aggregate risk profile. The 67.6% concentration ratio is the empirical anchor for that finding. Subsequent quarterly volumes will track whether business-associate concentration ratios, OCR queue dynamics, and detection-to-disclosure windows shift in response to the 2026 HIPAA Security Rule update, OCR enforcement priorities, and the propagation of upstream incidents into downstream covered-entity notifications. The series intends to be a constructive empirical resource for covered entities, business associates, regulators, policy researchers, and the broader healthcare cybersecurity community.

The next volume in this series will cover Q2 2026 and is scheduled for July 2026 publication.

9. Future Research Program

This inaugural issue establishes the analytical scope of the State of Compliance series and identifies three research gaps whose closure would materially strengthen the framework. Each is scoped below as a candidate for dedicated future work, either as quarterly-issue extensions or as dedicated working papers in the Secure Care Research Institute program.

9.1 A Proxy Layer for Threat Velocity

The decoupling claim central to this paper — that reporting velocity and threat velocity have diverged — rests on indirect signals. Direct measurement of threat velocity would require a proxy layer composed of at least the following time series, none of which is fully assembled in the current issue: ransomware leak-site publication volume by victim sector and month; CISA healthcare-sector advisory issuance frequency and severity distribution; dark-web PHI listing volume and pricing dispersion; and observed fraud claim rates against Medicare and private insurer populations, indexed against disclosed-breach populations. A Q2 2026 or dedicated working paper assembling these proxies would move the decoupling claim from qualitative inference to quantitative demonstration. The Patient Protect breach intelligence dashboard already indexes the leak-site and advisory streams among its seven sources; extracting the time series for publication is a bounded engineering task.

9.2 Quantifying the Business-Associate Concentration Dynamic

The business-associate concentration thesis — that upstream incidents disproportionately drive affected-population impact — is demonstrated in this issue through named cases (CareCloud, TriZetto, Conduent, IPPC) but is not quantified. A dedicated analytical extension would compute: (1) the percentage of total affected-population exposure in a given period that traces to upstream business associate or platform incidents versus direct covered-entity incidents; (2) the concentration ratio of exposure, expressed as the share of total affected individuals originating in the top N upstream incidents; (3) the downstream-propagation coefficient, expressed as the average number of covered-entity notifications produced per business associate incident; and (4) the time-to-propagation distribution from upstream disclosure to downstream covered-entity notification. These metrics would turn the concentration claim from structural observation into measurable sector characteristic, and would directly inform the regulatory recommendations in §7.3 regarding business associate oversight.

9.3 From Explanatory to Predictive TARF

The Transparency-Adjusted Risk Function in its current form is explanatory. It frames the Q1 2026 record, it identifies which lever moved in which direction, and it generates hypotheses. It does not yet forecast. A predictive TARF would require: (1) a time-series treatment of each of the four component indices (DMVI, AAF, HTI, R) at quarterly or monthly resolution; (2) validation against subsequent observed outcomes — specifically, whether period-t TARF values predict period-t+1 affected population, breach cost, or litigation volume; (3) scenario simulation capability enabling counterfactual analysis of policy interventions (the effect of a shortened notification window; the effect of Security Rule finalization; the effect of OCR budget change); and (4) uncertainty quantification appropriate to a framework whose component inputs are themselves estimates rather than measurements. This is not a quarterly-issue extension. It is a dedicated working paper, and the natural sequel to the current State of Compliance inaugural and the two prior Secure Care Research Institute papers.

Scoped as such, it would be the first healthcare-specific cybersecurity risk framework with demonstrated predictive validity — a positioning that the current paper cannot yet claim.

These three research directions are not in tension with the claims made in this paper. They are the natural empirical and methodological extensions of its framework. Naming them explicitly — rather than leaving them as unstated limitations — is consistent with the methodological posture established in §5 and Appendix B: where quantitative re-measurement is not performed, the research program should be transparent about what measurement would look like if attempted.

References

Perrin, A. (2025a). The economics of ePHI exposure: A long-term impact model of healthcare data breaches. Secure Care Research Institute, Patient Protect LLC. SSRN Working Paper 5257628. https://papers.ssrn.com/abstract=5257628

Perrin, A. (2025b). The cyber-economic stack: How AI turns healthcare data into a financialized attack asset. Secure Care Research Institute, Patient Protect LLC. SSRN Working Paper 5792382. https://papers.ssrn.com/abstract=5792382

Patient Protect. (2026). Breach intelligence dashboard: Seven sources, twelve analytical views. Patient Protect LLC. https://patient-protect.com/breachdash

HHS Office for Civil Rights Breach Portal. (2026). Notice to the secretary of HHS breach of unsecured protected health information [breach records for 2025–Q1 2026, accessed April 2026]. U.S. Department of Health and Human Services. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

HHS Office for Civil Rights. (2024, December 27). HIPAA Security Rule notice of proposed rulemaking to strengthen cybersecurity for electronic protected health information. U.S. Department of Health and Human Services.

HHS Office for Civil Rights. (2026, February). OCR launches Part 2 civil enforcement program [announcement]. U.S. Department of Health and Human Services.

calHIPAA. (2026a, March 9). January 2026 healthcare data breach activity and cybersecurity incidents. Calculated HIPAA. https://www.calhipaa.com/january-2026-healthcare-data-breach-activity-and-cybersecurity-incidents/

calHIPAA. (2026b, April). February 2026 healthcare data breach activity. Calculated HIPAA.

calHIPAA. (2026, February 15). December 2025 healthcare data breach report. Calculated HIPAA.

TechTarget / HealthITSecurity (Xtelligent). (2026, February 17). OCR launches Part 2 civil enforcement program, new breach portal features. TechTarget / Xtelligent Healthcare Media.

TechTarget / HealthITSecurity (Xtelligent). (2025, December). Largest healthcare data breaches reported to OCR in 2025. TechTarget / Xtelligent Healthcare Media.

Bank Info Security (ISMG). (2025, December 30). 2025 in health data breaches and predictions for 2026. Information Security Media Group.

Patient Protect Breach Intelligence Dashboard. (2026). Multi-source healthcare breach compilation [Q1 2026 data export]. Patient Protect LLC. https://patient-protect.com/breachdash

Oregon Attorney General. (2026). Consumer Information Protection Act breach notifications [TriZetto, QualDerm, Healthcare Interactive, Insightin Health]. Oregon Department of Justice.

California Attorney General. (2026). Data breach notifications [Insightin Health, Stockton Cardiology, Couve Healthcare]. California Department of Justice.

Vermont Attorney General. (2026, January 28). Insightin Health Data Breach Notice to Consumers. Office of the Vermont Attorney General.

HCIactive (Healthcare Interactive, Inc.). (2026). Notice of security incident [substitute breach notice]. Healthcare Interactive, Inc.

Insightin Health, Inc. (2026, January 28). Notice of a data privacy event. Insightin Health, Inc.

Comparitech. (2026, March 23). Insightin Health warns 142,000+ people of data breach claimed by ransomware group [updated to 1,144,686]. Comparitech.

DataBreaches.net. (2026, March 11). Insightin Health discloses its second data security incident in two years. DataBreaches.net.

This Week Health. (2026, February 2). Healthcare Interactive Data Breach Exposes 3.1 Million Patients Nationwide.

idstrong.com. (2026, March 19). Healthcare Interactive Data Breach Exposes 3 Million Patient Records.

InsuranceNewsNet. (2026, March 18). Massive Data Breach at Healthcare Interactive Affects Over 3 Million.

Morningstar. (2026, January 28). Insightin Health, Inc. Provides Notice of a Data Privacy Event.

WIS-TV. (2026, January 9). Personal medical data possibly exposed in Healthcare Interactive, Inc. data breach.

Fox News. (2026). Healthcare cyberattack hits TriZetto, 3.4 million affected.

Reed Smith. (2026, February 18). Two Breach Reports to OCR for Same Data Breach? OCR Begins Part 2 Compliance Enforcement Program.

Paubox. (2026a, April). Stockton Cardiology reveals ransomware breach as GENESIS claims 645GB stolen. Paubox Inc.

Paubox. (2026b, April). IPPC breach affects 133,862 people across long-term care network. Paubox Inc.

Paubox. (2026c). HIPAA breach analytical reports [monthly OCR-derived]. Paubox Inc.

Paubox. (2025). Healthcare breach analytical reporting and OCR investigation-queue tracking. Paubox Inc.

Becker's ASC Review. (2026, March 9). California cardiology group suffers data breach. Becker's Healthcare.

Cole & Van Note. (2026, April). IPPC data breach investigation. Cole & Van Note Attorneys at Law.

Security Magazine. (2026, February 17). Top 20 healthcare data breaches of 2025. BNP Media.

Alston & Bird. (2026, February 19). A new day for OCR's data breach portal: Are you ready? Alston & Bird Health Care Advisory.

Hunton Andrews Kurth. (2026, March 2). HHS OCR settles HIPAA Security Rule investigation with Top of the World Ranch Treatment Center for $103,000. Privacy and Cybersecurity Law Blog.

Paul Hastings. (2025, January 22). HHS OCR releases proposed updates to HIPAA Security Rule. Paul Hastings LLP.

BDO. (2025). Proposed HIPAA Security Rule updates. BDO USA.

Lexology. (2026, March 10). 3 must-know changes in the new HIPAA Security Rule NPRM.

Medcurity. (2026). HIPAA Security Rule changes in 2026: What you need to know.

Johnson Lambert. (2025, September 29). HIPAA's security shake-up: Mandatory controls and enhanced enforcement for 2025.

The Lyon Firm. (2026, March 28). Stockton Cardiology data breach: What California patients need to know.

RedPacket Security. (2026, February 17). [GENESIS] — Ransomware victim: Stockton Cardiology Medical Group.

ClaimDepot. (2026). IPPC data breach affects 133k exposing sensitive personal and health info.

Mass.gov. (2026). IPPC, Inc. individual consumer notification letter. Massachusetts Office of Consumer Affairs and Business Regulation.

Zeron. (2026, April). Healthcare data breach 2026: What 4 breaches reveal. Zeron Cyber Risk Intelligence.

Pindrop Security. (2025). Voice intelligence and security report: Healthcare sector threat trends. Pindrop Security Inc.

Intel 471, Recorded Future, and Flashpoint. (2024–2025). Dark web PHI pricing observations [aggregated]. As reported in Perrin (2025b).

HHS HC3 (Health Sector Cybersecurity Coordination Center). (n.d.). Intelligence briefing update: Dark web PHI marketplace. U.S. Department of Health and Human Services. As reported in Applied Tech (2025).

IBM X-Force. (2025). Healthcare data breach cost analysis: Pricing intelligence for dark web markets. IBM Corporation.

Total Assure. (2025, October). Healthcare cybersecurity statistics 2025.

Applied Tech. (2025, January 29). The black market for your unprotected healthcare information is exploding.

Medical Economics. (2026, April). False Claims Act recoveries hit a record $6.8 billion in 2025: DOJ National Healthcare Fraud Takedown charged 324 defendants with $14.6B intended loss.

TruthScan. (2025, November 6). AI-driven fraud in global healthcare: 2025 trends and countermeasures.

Keller Grover. (2026). AI and healthcare fraud: How artificial intelligence is being used to defraud Medicare.

IBM Security & Ponemon Institute. (2024). Cost of a data breach report. IBM Corporation.

Ponemon Institute. (2024). Healthcare data breach detection and response benchmarks. Ponemon Institute LLC.

Appendix A. Q1 2026 Healthcare Breach Inventory — Named Incidents

The following table inventories named healthcare-sector breaches with Q1 2026 public disclosures. The list is not exhaustive; it represents incidents that met either an affected-population threshold or a structural significance criterion for inclusion in the analytical section of this paper. Incidents with disclosure dates in Q1 2026 but incident dates in prior periods are included and marked. Affected-population figures are as publicly reported at the time of disclosure and may be subsequently revised.

Entity	Disclosure	Attack Type	Affected	Archetype / Note
TriZetto Provider Solutions	Feb 11 (OR AG) / Mar 3 (OCR)	Hacking/IT	3,433,965	BA cascade
QualDerm Partners, LLC	Feb 23 (OR AG) / Mar 23 (OCR)	Hacking/IT	3,117,874	Specialty aggregator
Healthcare Interactive (HCIactive)	Sep 22, 2025 / Jan 7, 2026 (OR AG)	Hacking/IT	3,056,950	BA cascade
Insightin Health, Inc.	Mar 5, 2026 (OR AG)	Ransomware (MEDUSA)	1,144,686	BA cascade
Illinois Dept. of Human Services	Feb 4, 2026	Unauth. Access/Disclosure	705,017	Direct (gov)
ApolloMD Business Services	Feb 11, 2026	Ransomware (Qilin)	626,540	BA cascade
Northwest Radiologists / Mt. Baker Imaging	Jan 29, 2026	Hacking/IT	362,713	Direct intrusion
Navia Benefit Solutions (Bellevue)	Mar 18, 2026	Hacking	319,208	BA cascade
Minnesota Dept. of Human Services	Jan 22, 2026	Unauth. Access/Disclosure	303,965	Direct (gov)
Harbor (OH)	Jan 20, 2026	Hacking/IT	216,000	Direct intrusion
Expert MRI	Jan 30, 2026	Hacking/IT	209,560	Direct intrusion
Modernizing Medicine, Inc.	Jan 13, 2026	Hacking/IT	198,795	Direct intrusion
Vikor Scientific, LLC	Feb 6 (OR AG) / Mar 2 (OCR)	Hacking/IT	139,964	Direct intrusion
Stockton Cardiology Medical Group	Feb 17, 2026 (GENESIS leak)	Ransomware (GENESIS)	Undisclosed (645 GB)	Named-group ransomware
Innovative Pharmacy Packaging Corp	Feb 27, 2026 (notice) / Apr 8, 2026 (OCR)	Hacking/IT	133,862	Detection-gap (OCR record outside Q1 — see §4.6)
Stryker Corporation	Mar 20–23, 2026 (public reporting)	Open-source attribution: Iran-linked	Medical device infra.	Nation-state — modeled-channel reference, see §4.5
CareCloud	Late Mar 2026 (public reporting)	Unauthorized access	Under investigation	Platform — modeled-channel reference, see §4.1
Mirra Health (FL Medicare members)	Late Mar 2026 (public reporting)	Offshore data mishandling	Undisclosed	Offshore archetype — modeled-channel reference, see §4.4

Appendix B. Reconciliation — OCR-Only vs Multi-Source Dashboard

This appendix reconciles the OCR-only Q1 2026 view (118 breaches affecting 9,651,076 individuals across January and February only, with March essentially absent at the time of late-March 2026 access) against the Patient Protect Dashboard's multi-source view (207 unique deduplicated and healthcare-sector-scoped breaches affecting approximately 15.9 million individuals across the full Q1 quarter, drawn from a late-April 2026 dashboard export). The reconciliation has four structural components: (a) March 2026 incidents surfaced through state attorney general channels and continued OCR backlog clearance, (b) affected-population revisions on incidents whose OCR placeholder filings were updated through state-level disclosures, (c) deduplication of multi-state filings into single canonical incident records, and (d) exclusion of records outside healthcare-sector scope.

Reconciliation component	Mechanic	Effect on incident count	Effect on affected
OCR-only baseline (late-March 2026 access)	HHS OCR portal as accessed late-March 2026	118 (Jan 46 + Feb 63 + Mar 2 + 7 late-arriving)	9,651,076
+ March 2026 multi-source	State AG filings + continued OCR backlog clearance through late-April	+78 (80 Mar dashboard – 2 OCR-only Mar)	March component net of dedup
+ Affected-population revisions	OCR placeholders revised via state-level filings (e.g., HCIactive 501 → 3,056,950)	0 (existing incidents)	+~6.2M post-revision
+ State-level coverage	Oregon AG, California AG, etc. capturing pre-OCR filings	Subsumed in March count above	Concentrated in upstream BAs
– Multi-state filing dedup	Same entity filed in multiple states + HHS OCR collapsed to single record	–7 (218 raw → 211 deduplicated)	0 (dedup retains max)
– Healthcare-sector scope filter	4 records outside healthcare sector excluded (financial advisory, hospitality, plaintiff law)	–4 (211 → 207)	–4,658
– Dashboard Feb HHS OCR ingestion lag	Estimated 1–3 week dashboard lag behind OCR portal	–16 implicit (Feb dashboard 47 vs OCR 63 at late-March)	Component of QA gap, see App. D
= Multi-source Q1 2026 (this paper)	**Patient Protect Dashboard, deduplicated and scoped, late-April 2026 export**	**207 unique healthcare breaches**	**15,894,271**

Three reconciliation components warrant explicit acknowledgment. First, the dashboard's February count (47) is lower than the OCR-only February count (63 at late-March access), reflecting an estimated 1–3 week dashboard ingestion lag behind the OCR portal. Appendix D documents this gap as the principal known data-quality limitation for Q1 2026 and commits to a Q2 2026 reconciliation. Second, the breach-by-breach OCR-portal date-added timestamps are not published, so an entity-by-entity reconciliation of which OCR portal entries were added between late-March and late-April 2026 is not currently possible from public sources. The Q2 2026 issue of this series will reconcile both the February gap and the late-arrival entity list against the OCR portal at the Q2 access date. Third, the healthcare-sector scope filter excluded four records (Brown Advisory LLC, Drivestream Inc., Pyramid Global Hospitality, Wisner Baum LLP) where the entity's primary business is outside healthcare and no business-associate relationship to a covered entity is evident from the available filing detail; this is documented in Appendix D and is consistent with the paper's healthcare-sector restriction stated in §1. The full reconciliation methodology, including the deduplication logic, source-channel attribution rules, scope-filter criteria, and revision-handling policy, is documented in Appendix D. The compilation methodology is proprietary to Patient Protect LLC; the underlying primary-source records are publicly accessible.

Appendix C. Methodology Notes and Limitations

The State of Compliance series adopts a dual-source methodology in which formal regulatory data (the HHS OCR breach portal) is complemented by state attorney general notifications, FTC enforcement records, CISA advisories, CMS enforcement data, community intelligence, and modeled threat signals. This multi-source approach is necessary because no single source captures the full breach record in real time.

Incident classification into the seven archetypes described in §4 is performed using a structural-attribute logic rather than a first-public-label logic. An incident that was publicly described as ransomware but structurally represents a business associate platform cascade is classified under §4.1, not §4.2. This classification logic is stable across quarters and allows year-over-year comparison of archetype distribution independent of reporter vocabulary drift.

Affected-population figures are reported at the most recent publicly available value. In many cases these figures are subsequently revised upward as investigations proceed; revisions discovered after paper publication will be reflected in the subsequent quarterly volume rather than in silent back-edits to this paper.

This issue applies the TARF framework qualitatively. A fully quantitative recalculation of DMVI, AAF, HTI, and R for Q1 2026 is beyond the scope of this issue and is a candidate for a dedicated future working paper. Where this paper characterizes TARF components directionally in Q1 2026 (§5), it relies on structural reasoning and publicly observable signals rather than primary measurement.

Financial and epidemiological impact estimates derive from the source models in Perrin (2025a, 2025b) and are not re-derived here. Specifically, the $8–12 billion annual fraud-suppression estimate referenced in §7.3 is a modeled output of prior research rather than an observed savings number; it depends on prior-paper assumptions about DMVI, AAF, and downstream fraud yield. It is reported in scale-validation context against independent 2025 figures (the $14.6 billion DOJ takedown alleged intended loss; the $68 billion total annual healthcare fraud estimate) but should not be treated as independent empirical evidence of the specific suppression figure.

Distinctions between observed data, modeled outputs, and directional inferences are maintained throughout the paper. As a summary:

Observed data in this paper includes: breach counts at OCR-only late-March access (46 Jan, 63 Feb, 2 Mar 2026) and at multi-source late-April access (80 Jan, 47 Feb, 80 Mar 2026, post-dedup, post-scope-filter); affected-population totals; named-incident timelines with cited sources (Stockton, IPPC, QualDerm, Healthcare Interactive, Insightin, TriZetto, etc.); OCR investigation queue figures (882, 978); regulatory event dates (Part 2 enforcement, TOTW settlement, NPRM publication, regulatory freeze EO).

Modeled outputs referenced in this paper include: DMVI $280–310/record (derived from 2024–25 primary observations in prior research; not re-measured for Q1 2026); AAF 1.18–1.30 (derived from 2022–24 modeling in prior research; not re-measured for Q1 2026); the $8–12B suppression estimate (derived from combined DMVI/AAF/latency modeling in prior research); HTI healthcare 23 / finance 81 (derived from prior-research cross-sector scoring, not re-computed).

Directional inferences drawn in this paper — most notably that the Q1 2026 record is directionally consistent with increased sector exploitability despite the declining breach count, and that threat velocity and reporting velocity have moved out of alignment — are inferences from combined observed and modeled inputs rather than direct measurements. The paper labels these inferences consistently with the word "directionally" and describes

the framework application as "qualitative."

Additional limitations specific to this inaugural issue: (1) The March 2026 OCR reporting gap is material and is acknowledged throughout. Figures that rely on Jan–Feb OCR reporting are labeled as such. (2) Dark-market PHI pricing (DMVI) is not re-measured for Q1 2026; the 2024–2025 baseline from Perrin (2025b) is the working assumption, corroborated on scale by independent 2025 sources (HHS HC3; IBM X-Force, 2025; Total Assure, 2025). (3) HTI is not re-computed; directional movement is inferred from observable signals. (4) Some named-incident characterizations (for example, "insider" for Weill Cornell; "Iran-linked" for Stryker) rely on second-hand reporting or probabilistic attribution rather than primary entity disclosure; these are flagged where they occur. (5) Several named incidents in Appendix A were identified in public reporting but did not carry published affected-population figures at the time of this paper's preparation; these are marked "Undisclosed." (6) The paper does not evaluate or rank any specific compliance software or consulting vendor. (7) All framework-based directional claims are, by construction, hypothesis-generating rather than hypothesis-testing; the Q2 2026 issue of this series will be the first opportunity to evaluate whether the Q1 directional claims are supported by subsequent data. (8) No Q1 2026 named breach in Appendix A has been publicly attributed to an AI-enabled primary attack vector; AAF-related discussion in §5.2 relies on independent industry evidence of AI-enabled healthcare fraud in 2025 rather than direct Q1-incident linkage.

Appendix D. Multi-Source Dashboard QA and Validation Notes

The Q1 2026 empirical record presented in this paper rests on the Patient Protect Breach Intelligence Dashboard, a proprietary multi-source compilation maintained by Patient Protect LLC. This appendix documents the QA and validation procedures applied to the dashboard's Q1 2026 record, the deduplication logic, the channel composition, and the known limitations of the current data infrastructure. The compilation methodology, dedup logic, channel composition algorithm, and underlying data architecture are proprietary intellectual property of Patient Protect LLC. The underlying source records are public; the proprietary layer consists of source normalization, deduplication, channel attribution, and dashboard architecture. The headline findings of this paper, including the 67.6% concentration ratio, can be independently verified against publicly accessible primary disclosures (see D.7).

D.1 Source Channel Composition for Q1 2026

The dashboard ingests breach intelligence from seven primary channels: HHS Office for Civil Rights breach portal, state attorney general filings, FTC enforcement records, CISA advisories, CMS enforcement records, crowdsourced community intelligence, and modeled threat signals. For Q1 2026, after deduplication of multi-state filings and exclusion of records outside healthcare-sector scope, the dashboard contains 207 unique breach incidents reported January 1 through March 31, 2026.

Of these 207 unique incidents, 169 carry primary attribution to the HHS OCR breach portal (approximately 4.59M affected) and 38 carry primary attribution to a state attorney general filing (approximately 11.30M affected, with Oregon contributing the substantial majority by affected-population total, followed by Washington, California, and Indiana). Modeled threat signals, FTC enforcement records, CISA advisories, CMS enforcement records, and crowdsourced community intelligence did not contribute primary-source breach records to the deduplicated Q1 2026 healthcare set; the dashboard's modeled-threat-signal channel surfaced contextual references for several incidents (notably Stryker, CareCloud, and Mirra Health, see §4) which are referenced in this paper for archetype illustration but excluded from the deduplicated 207-incident analytical dataset.

Several of the 207 unique deduplicated incidents have filings in multiple channels (for example, an Oregon AG filing and a corresponding HHS OCR portal entry); the dashboard's primary-channel attribution rule retains the channel that produced the originating disclosure, but the existence of cross-channel filings means the raw record counts in each channel sum to more than 207. Multi-state filings collapsed during deduplication are documented in D.2.

The state-level channel disproportionately drives the affected-population total relative to its share of incident count. The four largest Q1 2026 incidents (TriZetto, QualDerm, Healthcare Interactive, Insightin Health), together accounting for 67.6% of all Q1 affected individuals, were sourced through state attorney general filings (principally Oregon AG) before the corresponding HHS OCR portal entries appeared. The pattern is the empirical justification for multi-source compilation as the operating methodology of this series.

D.2 Deduplication Logic and Audit

Multi-state filings produce duplicate dashboard entries when the same incident is reported separately to multiple state attorney general offices in addition to HHS OCR. The dashboard's deduplication logic operates on normalized entity name: entity names are lowercased, punctuation is stripped, and whitespace is collapsed; records that share a normalized entity name are then treated as filings of the same incident. Among matched records, the dashboard retains the row carrying the highest reported affected-population value, on the working assumption that later state-level filings or revised OCR entries contain more complete population counts than initial placeholders. This is a conservative collapse rule that prioritizes the most complete population data for each unique incident.

For Q1 2026, the raw dashboard contained 218 records meeting the breach-class and Q1-reporting-date filters. Normalized-entity-name dedup collapsed 7 multi-state pairs into 7 single records, producing 211 unique breaches. A

subsequent healthcare-sector scope filter excluded 4 records (described in D.2a below), yielding the final 207-incident analytical dataset.

The 7 collapsed multi-state pairs are TriZetto Provider Solutions (Oregon AG + HHS OCR Missouri filing, both carrying 3,433,965 affected); QualDerm Partners (Oregon AG + HHS OCR Tennessee filing, both at 3,117,874); Vikor Scientific (Oregon AG + HHS OCR South Carolina filing, both at 139,964); Expert MRI (HHS OCR California carrying 209,560 + California State AG with no published affected count); Blue Shield of California (two HHS OCR rows at 607 and 93,921, both same-day same-vector — see edge-case discussion in D.8); BlueCross BlueShield of Tennessee (two HHS OCR rows at 1,670 and 780, both same-day, different vectors — see D.8); and Couve Healthcare Consulting LLC DBA Evergreen Healthcare Group (HHS OCR Washington carrying 11,795 + California State AG with no published affected count).

D.2a Healthcare-sector scope filter

Following deduplication, four records were excluded from the analytical dataset on healthcare-sector scope grounds: Brown Advisory LLC (financial advisory, 2 affected); Drivestream Inc. (IT consulting, 505 affected); Pyramid Global Hospitality (hotel management, 3,434 affected); and Wisner Baum LLP (plaintiff law firm, 717 affected). Each of these entities was filed with a state attorney general under a state breach notification statute, but each operates outside the healthcare sector and no business-associate relationship to a covered entity is evident from the filing detail available at the dashboard ingestion date. Total exclusions: 4 incidents and 4,658 affected individuals. The decision rule for inclusion in the State of Compliance series, stated in §1, is U.S. healthcare-sector breaches affecting covered entities, business associates, or upstream platform vendors whose data products serve healthcare organizations. State AG filings whose subject entity does not meet this threshold are excluded.

The full edge-case discussion of where dedup and scope decisions face known limits is in D.8.

D.3 Reconciliation: HHS OCR-Only vs Multi-Source

The 118-breach OCR-only count cited in §3.1 reflects the OCR portal as accessed in late March 2026. The 169-breach OCR-attributed count in the deduplicated and scoped dashboard reflects continued OCR backlog clearance through the late-April 2026 dashboard export. The 51-breach difference (169 - 118) corresponds to OCR portal entries added between late-March and late-April 2026, including (a) further January and February incidents that arrived after the late-March cutoff, and (b) March 2026 incidents that began appearing in the OCR portal as the backlog cleared.

The dashboard's February 2026 count (47 breaches post-dedup, post-scope-filter) is lower than the OCR-only late-March February count (63 breaches). The gap is the dashboard's principal known data-quality limitation for Q1 2026 and reflects the dashboard's HHS OCR ingestion lag of an estimated 1–3 weeks. Some OCR-portal February records present in the OCR portal as of late March 2026 had not yet been ingested into the dashboard at the late-April export. The Q2 2026 issue will reconcile this gap by re-running the Q1 2026 dataset against the OCR portal at the Q2 access date.

D.4 Data Quality Flags and Known Issues

The Q1 2026 final analytical dataset (207 incidents) contains the following flagged records: 14 records with NaN affected-population values, of which 12 are California State AG filings whose published format does not consistently include affected-population counts in the dashboard's ingestion pattern (the remaining 2 are an Indiana State AG filing for Ascension St. Vincent and a Washington State AG filing for Guardian Pharmacy of Washington); approximately 27 records with affected-population values of 500 or 501 (placeholder figures pending review completion under HIPAA Breach Notification Rule reporting practice); and a small number of records with vector classified as "Unknown" pending further information.

These flagged records are retained in the deduplicated dataset because their incident-level existence is independently verifiable from the source channel even when affected-population data is incomplete. Affected-population aggregations in this paper exclude NaN-valued records from the sum but include them in the incident-count denominator (207). The California-concentrated NaN pattern reflects a specific dashboard-ingestion limitation rather than an absence of underlying data: the underlying California State AG filings exist and contain disclosure information, but the dashboard's California ingestion pipeline does not currently capture affected-population values at the same rate as Oregon and Washington filings. The Q2 2026 issue will address this with an enhanced California ingestion pass.

D.5 Cross-Validation Against External Sources

The four largest Q1 2026 incidents have been independently verified against external secondary sources beyond their primary state AG and HHS OCR filings. TriZetto Provider Solutions (3,433,965 affected) is corroborated by Bank Info Security (2025) and Fox News (2026). QualDerm Partners (3,117,874 affected) is corroborated by primary state AG filings in Oregon and Tennessee. Healthcare Interactive / HCIactive (3,056,950 affected) is corroborated by Paubox (2026), This Week Health (2026), Comparitech (2026), Morningstar (2026), idstrong.com (2026), InsuranceNewsNet (2026), and WIS-TV (2026). Insightin Health (1,144,686 affected) is corroborated by DataBreaches.net (2026), Comparitech (2026), the California Attorney General's office (2026), and the Vermont Attorney General's office (2026).

D.6 Roadmap to Reliable Reporting Infrastructure

The State of Compliance series has, as one of its operating commitments, the maturation of multi-source healthcare breach compilation from craft toward auditable reporting infrastructure. Q1 2026 is the inaugural application; subsequent issues will document and address the limitations identified above. Specific Q2 2026 deliverables include: (1) reconciliation of any Feb 2026 OCR records absent from the dashboard's Q1 ingestion; (2) entity-by-entity reconciliation of late-arriving OCR portal additions, with date-added timestamps where available; (3) extension of the deduplication logic to handle staggered affected-population revisions across sources; (4) publication of dashboard channel-coverage statistics at the state level to identify under-covered jurisdictions; (5) documentation of any new source channels added to the dashboard between Q1 and Q2 2026.

D.7 Reproducibility and Independent Verification

The empirical claims in this paper rest on a proprietary compilation, but the underlying primary records are publicly accessible and the headline findings can be independently verified from source. A reader who wishes to verify the central claim of this paper — that four upstream business associate or platform-vendor incidents drove approximately 67.6% of Q1 2026 affected individuals — can do so as follows.

For TriZetto Provider Solutions (3,433,965 affected): the Oregon Department of Justice maintains a public consumer information protection breach notification database; TriZetto's filing was dated February 11, 2026. The corresponding HHS OCR portal entry under "Cognizant TriZetto" is publicly searchable on the HHS OCR breach portal (ocrportal.hhs.gov/ocr/breach), filed approximately March 3, 2026. Independent secondary corroboration: Bank Info Security (December 30, 2025); Fox News (March 2026 coverage).

For QualDerm Partners, LLC (3,117,874 affected): the Oregon Attorney General's filing was dated February 23, 2026; the HHS OCR portal entry followed approximately March 23, 2026, under "QualDerm Partners, LLC" filed in Tennessee. The QualDerm intrusion window of December 23–24, 2025 is documented in the entity's primary disclosure notice.

For Healthcare Interactive, Inc. / HCIactive (3,056,950 affected): the entity filed an initial HHS OCR portal report on September 22, 2025 using a placeholder figure of 501 individuals. The Oregon Attorney General was notified of the revised figure of 3,056,950 individuals on January 7, 2026. State attorney general filings additionally exist in California, Maine (87,565 individuals), South Carolina (103,000 individuals), Texas, Vermont, Massachusetts, and New Hampshire. Independent secondary corroboration: This Week Health (February 2, 2026); Paubox (March 3, 2026); Comparitech; Morningstar (January 28, 2026); idstrong.com; InsuranceNewsNet; WIS-TV (January 9, 2026).

For Insightin Health, Inc. (1,144,686 affected): the California Attorney General sample notice is publicly available at oag.ca.gov; the Vermont Attorney General notice was filed January 28, 2026 (ago.vermont.gov). The Oregon Attorney General website added the figure of 1,144,686 on or around March 23, 2026. The MEDUSA ransomware leak-site posting from September 26, 2025 is documented in DataBreaches.net coverage and Comparitech reporting (March 23, 2026).

The 67.6% concentration ratio is the sum of these four publicly-verifiable affected-population figures (10,753,475) divided by the dashboard's deduplicated and healthcare-sector-scoped Q1 2026 affected-population total (15,894,271). The arithmetic: 10,753,475 / 15,894,271 = 0.67658, rounded to 67.6%. A reader who reproduces only the four upstream concentrators against publicly available primary sources will confirm the numerator. The denominator depends on the dashboard's full multi-source compilation, which the paper acknowledges as proprietary; two independent denominator-substitution checks demonstrate the finding's robustness:

(a) Substituting the OCR-only late-March 2026 denominator (9,651,076 across 118 January–February breaches) yields a top-4 share of 111.4%, which is mechanically meaningless because three of the four headline incidents had not yet been filed with HHS OCR at the late-March access — but it confirms the directional point that OCR-only reporting at that access date materially undercounted both numerator and denominator.

(b) Substituting the unscoped 211-incident dataset denominator (15,898,929, prior to healthcare-sector scope filter exclusions) yields 10,753,475 / 15,898,929 = 67.64%, identical to two decimal places.

The concentration finding is robust to the scope-filter decision; it would survive an aggressive 10-15% upward revision of the denominator (see D.9).

D.8 Known Limitations of the Deduplication Logic

The current deduplication algorithm — exact match on normalized entity name plus exact match on affected-population value — is conservative and produces stable, auditable results, but it has identifiable failure modes that warrant explicit acknowledgment.

First, slight variations in affected-population values can prevent appropriate collapse. If TriZetto were filed with the Oregon AG at 3,433,965 individuals and with HHS OCR at 3,433,902 individuals (after a minor data review revision), the current logic would treat the two records as separate incidents rather than collapsing them. The Q1 2026 dataset did not exhibit this pattern at material scale; the Q2 2026 issue will introduce a tolerance threshold (likely +/-1.0% on affected-population) for entities whose normalized names match.

Second, name normalization can fail when entities operate under variant legal names or DBA structures. The Q1 2026 dataset contained two examples (Vikor Scientific, LLC vs Vikor Scientific, LLC. with a trailing period; Couve Healthcare Consulting, LLC DBA Evergreen Healthcare Group with two state filings) where the current logic handled the variants correctly but not robustly. Future versions of the normalization algorithm will incorporate fuzzy entity matching (Levenshtein-distance based) with manual review for proposed collapses.

Third, the same root incident may produce different affected-population counts when filed by an upstream business associate versus a downstream covered entity. The TriZetto incident is the canonical example: TriZetto itself filed at 3,433,965 individuals as the entity that experienced the breach, while OCHIN, an affected covered-entity client of TriZetto, separately reported approximately 700,000 affected patients to HHS OCR. The current logic treats these as separate records, which is correct under HIPAA's reporting obligations (each entity has independent notification duties) but produces an apparent over-count when readers attempt to sum incident-level affected populations. The methodology section (§2) and §3.2 both acknowledge this asymmetry; the dashboard does not currently distinguish "originating incident" from "downstream notification" at the data-row level, and that distinction is a Q2 2026 deliverable.

Fourth, the deduplication logic does not attempt to reconcile differences across source channels in incident metadata other than entity name and affected-population (for example, vector classification, breach date, discovery date). Where a multi-state filing reports the same entity and same affected count but different vector classifications, the dashboard retains the earliest-dated record's vector field; subsequent fields from later records are not merged.

Fifth, the current dedup rule (entity-name match → keep highest affected) can over-collapse in a specific edge case: when the same entity files two genuinely distinct breach reports on the same day, both filings collapse and the smaller one is dropped. Two such cases appeared in the Q1 2026 raw data: Blue Shield of California (two HHS OCR rows on January 7, 2026 with 607 and 93,921 affected respectively, same vector) and BlueCross BlueShield of Tennessee (two HHS OCR rows on March 2, 2026 with 1,670 and 780 affected, different vectors). In both cases the dashboard kept the higher-affected row. If these are in fact two distinct breach reports rather than amended versions of a single report, the true Q1 incident count would be 209 rather than 207, and the affected-population total would be approximately 1,387 individuals higher. The directional effect on the 67.6% concentration ratio is below the rounding threshold (the two-decimal value would shift from 67.66% to 67.65%). The Q2 2026 issue will introduce a refinement that distinguishes "amended-filing same-day" from "distinct-incident same-day" pairs based on portal metadata not currently ingested.

These limitations are noted explicitly here, in advance of skeptical scrutiny, because the credibility of the multi-source approach depends on transparent acknowledgment of where the methodology has known seams.

D.9 Headline Numbers as Compilation Totals, Not Precise Claims

The headline figures cited in this paper — 207 unique Q1 2026 healthcare breaches affecting approximately 15.9 million individuals — are accurately characterized as the multi-source compilation totals at the late-April 2026 dashboard export, after deduplication and healthcare-sector scope filtering. They are not precise claims of unchanging fact, and three sources of variation should be expected to shift these totals modestly in subsequent quarters.

First, the multi-source compilation is itself a moving target. As OCR clears its investigation backlog and as state attorney general filings continue to land for Q1 2026 incidents, the dashboard will continue to ingest additional records and continue to revise affected-population counts upward where state-level filings update prior placeholders. The Q2 2026 issue is expected to reflect a Q1 2026 total that is somewhat higher than the figures presented here, both in incident count and in affected population.

Second, the deduplication logic, as it matures (per D.8), is expected to reduce the unique-incident total slightly by collapsing close-but-non-identical records that the current logic retains separately. The expected magnitude is small (low single digits of incidents in Q1) but non-zero.

Third, the affected-population total is more sensitive to revision than the incident count, because individual large incidents undergo upward revisions as data reviews complete. The Healthcare Interactive case (501 → 3,056,950, a 6,098× revision over four months) is an outlier in magnitude but representative in direction.

Readers should accordingly treat the 207 / 15.9M figures as best-available compilation totals at a specific access date rather than as precise immutable facts. The 67.6% concentration ratio is more stable, because it is anchored on four large incidents whose affected-population figures are now established at multi-state-confirmed values. Even if the denominator (full Q1 affected) revises upward by 10–15% in subsequent quarterly issues — an aggressive upward-revision scenario — the four upstream concentrators' top-share would remain in the 60–70% range. The concentration finding is robust across plausible data-revision scenarios.

The dashboard remains a proprietary instrument under continuous development. The compilation logic, dedup methodology, source-channel weighting, and analytical views described above are protected intellectual property of Patient Protect LLC, and the underlying compilation may constitute a protectable database under 17 U.S.C. §103. Licensing and methodology inquiries: research@patient-protect.com.

Suggested Citation

APA

Perrin, A. (2026). State of compliance: Q1 2026 healthcare breach review — Multi-source compilation and the concentration finding. The State of Compliance Series, Vol. 1, Issue 1. Secure Care Research Institute, Patient Protect LLC.

Chicago

Perrin, Alexander. "State of Compliance: Q1 2026 Healthcare Breach Review." The State of Compliance Series, Vol. 1, Issue 1. Working paper. Chicago: Secure Care Research Institute, Patient Protect LLC, 2026.

Copyright

Disclaimer

This paper does not constitute legal, compliance, or investment advice. Readers are responsible for independent verification of facts and for consultation with qualified counsel before acting on any statement contained herein. The Secure Care Research Institute is an independent research program operating under Patient Protect LLC; the views expressed are those of the author.

◆ ◆ ◆

END OF PAPER