The State of Compliance Series Vol. 1, Issue 2

State of Compliance

Q2 2026 Healthcare Breach Review

10 Verified Disclosures
At least 2.7M Affected
AI-Vendor Cascade Led Quarter
Multi-Source Compilation

PUBLISHED BY
Secure Care Research Institute
Patient Protect LLC

VERSION
1.1 · 2026

Abstract

This brief reports ten independently verified healthcare data breach disclosures submitted to the HHS Office for Civil Rights (OCR) breach portal during the second quarter of 2026 (April 1 through June 30), compiled and verified by the Secure Care Research Institute as of July 2, 2026. Read together, the verified record describes two distinct layers of the sector: breach impact concentrated upstream at a single large platform, while breach frequency remained distributed downstream across independent practices. Together, the ten disclosures establish a floor of at least 2,698,826 affected individuals for the quarter — a minimum grounded in individually confirmed incidents, not a comprehensive total, because a large share of the underlying multi-source compilation could not be independently verified to a defensible standard within this brief's cutoff. The largest verified disclosure, at Xsolis, Inc., an artificial-intelligence-enabled utilization-management vendor, continues the upstream data-aggregation pattern the series identified in its inaugural Q1 2026 issue. A second verified disclosure, at Radiology Associates of Richmond, documents a covered entity's second breach within roughly fifteen months. The brief applies the series' Transparency-Adjusted Risk Function to these findings, closes with recommendations for covered entities and business associates, and documents full source reconciliation, exclusion logic, and verification methodology in the appendices.

Keywords: HIPAA breach notification, upstream data aggregation, business associate risk, artificial intelligence vendor risk, repeat-victim governance, OCR breach portal, multi-source verification

Executive Summary

The defining pattern of Q2 2026, read across the verified record, is two-layered. Breach impact continues to concentrate upstream at a small number of large platforms — this quarter, an AI-enabled vendor rather than a claims-processing cascade. Breach frequency, distinct from impact, remains distributed downstream across the sector's independent practices. Every finding in this brief is an instance of one layer or the other, and the Key Takeaways below map each finding to its layer.

Ten Q2 2026 healthcare breach disclosures met this brief's verification standard: an OCR submission date confirmed within the April 1–June 30 window, and an affected-population figure corroborated by at least one source independent of the underlying compilation. Together they establish a floor of at least 2,698,826 affected individuals — a minimum grounded in confirmed incidents, not a claim about the quarter's true total, which the underlying compilation could not support to a defensible standard as of this brief's cutoff. Full methodology and the exclusion log are in the appendices; the finding that a defensible quarter total was not achievable is itself a documented result, not an omission.

Two findings anchor the issue. First, the upstream data-aggregation pattern identified in the Q1 2026 report continued. The quarter's largest verified disclosure, at the AI-enabled utilization-management vendor Xsolis, affected 1,396,519 individuals — 51.7% of the verified floor by itself, and more than five times the next-largest verified disclosure. Records belonging to a client that had ended its Xsolis relationship in 2021 were still present in the breach. Second, Radiology Associates of Richmond disclosed a second breach within roughly

fifteen months of its first — a governance pattern distinct from data-aggregation risk and worth tracking independently.

> **KEY FINDINGS**
>
> Ten verified Q2 2026 disclosures establish a floor of at least 2,698,826 affected individuals. Xsolis, an AI-vendor cascade, accounts for 51.7% of that floor and continues the Q1 upstream-aggregation pattern. Radiology Associates of Richmond's second breach in fifteen months is a distinct governance finding. Below these two, seven of the ten verified disclosures occurred at independent specialty or imaging practices rather than hospital systems or platform vendors — the volume of the verified set, as opposed to its largest incident, is concentrated at the sector's long tail.

This is a shorter issue than the inaugural Q1 2026 report by design, not by default: it reports only what could be independently verified, at the length that verification supports. The appendices document why a full quarter-level count was not achievable this issue and what would let a future issue return to that form.

Key Takeaways

1. Upstream concentration persisted, through a new channel. Q1's impact concentrated in four claims-processing and benefits-administration cascades; Q2's largest verified disclosure came from an AI-enabled utilization-management vendor (Xsolis, §1.1). The mechanism is unchanged — a small number of platforms aggregating data across hundreds of clients — but the type of platform is shifting toward AI.

2. Breach frequency, distinct from breach impact, sits downstream with independent practices. Seven of the ten verified disclosures occurred at small specialty or imaging practices (§1.4), not at the large platforms that drive impact. Both patterns are true at once and describe different layers of the same sector.

3. A repeat-victim governance pattern is worth tracking on its own. Radiology Associates of Richmond's second breach within roughly fifteen months (§1.2) is not a data-aggregation story; it is a remediation-completeness question this series will track into Q3.

4. Retention beyond operational need remains a standing exposure. Records from a Xsolis client that ended its vendor relationship in 2021 were still present in the 2026 breach (§1.1), a finding this brief ties directly to the TARF reusability component (§3).

5. The regulatory floor did not move. OCR continued to cite risk-analysis failures in every one of its April 2026 settlements (§4), independent of whether the proposed Security Rule update finalizes.

1. Anatomy of Q2: Verified Disclosure Archetypes

The ten verified disclosures are not interchangeable. Each represents a distinct structural pattern, and together they characterize the quarter more fully than any single lead incident can. Two archetypes carry the most

consequential findings; two more, visible only once the verified set reached ten entries, describe the shape of the record beneath them.

1.1 The AI-Vendor Cascade: Xsolis

Xsolis, an AI-driven utilization-management vendor whose platform is used by more than 600 hospitals and health systems, disclosed a breach affecting 1,396,519 individuals, reported to HHS OCR on June 5, 2026. The underlying incident was a phishing attack on or about January 20, 2026, detected January 22 and disclosed months later — a Q2 breach disclosure rather than a Q2-dated incident, a distinction this brief maintains throughout. Xsolis is the largest verified Q2 disclosure and, at more than five times the next-largest entry in the verified set, the clearest continuation of the upstream-aggregation pattern this brief could confirm. That comparison is bounded by the ten-incident verified set, not a claim about the full quarter's distribution, which this brief does not attempt to state.

That the quarter's largest verified disclosure came from an AI vendor — whose product function depends on aggregating clinical data across hundreds of clients — is a forward-looking signal about where concentration risk is migrating. The Q1 cascades ran through claims processors and benefits administrators; Q2's largest ran through an AI platform.

One detail in the Xsolis disclosure carries a specific operational lesson. Rochester Regional Health, a confirmed affected system, had ended its Xsolis relationship in 2021, yet approximately 18,600 of its patients' records were still present in the Xsolis environment at the time of the 2026 breach. Data that survives a vendor relationship without documented disposition remained exposed years after the business relationship that justified holding it had ended. Vendor offboarding should include documented confirmation of data return or destruction, and a retention schedule that defines when records are purged from each system.

> **VERIFIED LEAD INCIDENT**
>
> Xsolis, Inc. — 1,396,519 individuals, OCR-reported June 5, 2026. An AI utilization-management vendor serving 600+ hospitals. The largest verified Q2 disclosure, continuing the upstream-aggregation pattern through an AI platform. Records from a client that left in 2021 were still exposed.

1.2 The Repeat-Victim Pattern: Radiology Associates of Richmond

Radiology Associates of Richmond (266,183) disclosed a second breach within roughly fifteen months of its first, and the case is worth treating as a finding in its own right rather than a table entry. The Virginia imaging practice disclosed a first breach in April 2024, affecting more than 1.4 million patients and reported to OCR on July 1, 2025. A second, separate incident began around July 25, 2025 — within weeks of its first breach's federal reporting — and its disclosure is what places this entry in the Q2 2026 window: the practice's investigation concluded April 6, 2026, and notification letters began May 21, 2026, independently confirmed by SecurityWeek and DataBreaches.net against a matching OCR portal date.

The sequence raises a governance question distinct from the data-aggregation pattern in §1.1: whether the security gaps behind the first breach were fully remediated before the second occurred. Repeat breaches at a single covered entity within a short window raise that question directly. This brief does not have visibility into the practice's internal remediation record and does not assert that the gaps went unaddressed; the sequence is reported as a pattern worth tracking into future issues, not a finding of causation.

1.3 Named-Group Extortion

Three of the ten verified disclosures were claimed by named ransomware or extortion groups rather than disclosed as unattributed unauthorized access: Southern Illinois Dermatology (Insomnia, 160,312 affected), Western Orthopaedics (PEAR, 113,330 affected), and Hematology Oncology Consultants (Rhysida, 62,972 affected). Each group is independently active elsewhere in the 2025–2026 healthcare threat landscape. PEAR appears in public reporting as a newer extortion actor associated with data-exfiltration claims rather than traditional encryption-only ransomware. Rhysida has claimed credit for a series of healthcare-sector attacks since 2023, predominantly against hospital systems and specialty practices.

Named-group attribution does not change a covered entity's notification obligations, but it changes the operational calculus for affected individuals. Exfiltration-only groups such as PEAR create secondary exploitation risk immediately upon claim, independent of any ransom negotiation, because the data is already circulating rather than held for ransom.

Figure 1. Vector Attribution Across the Verified Set

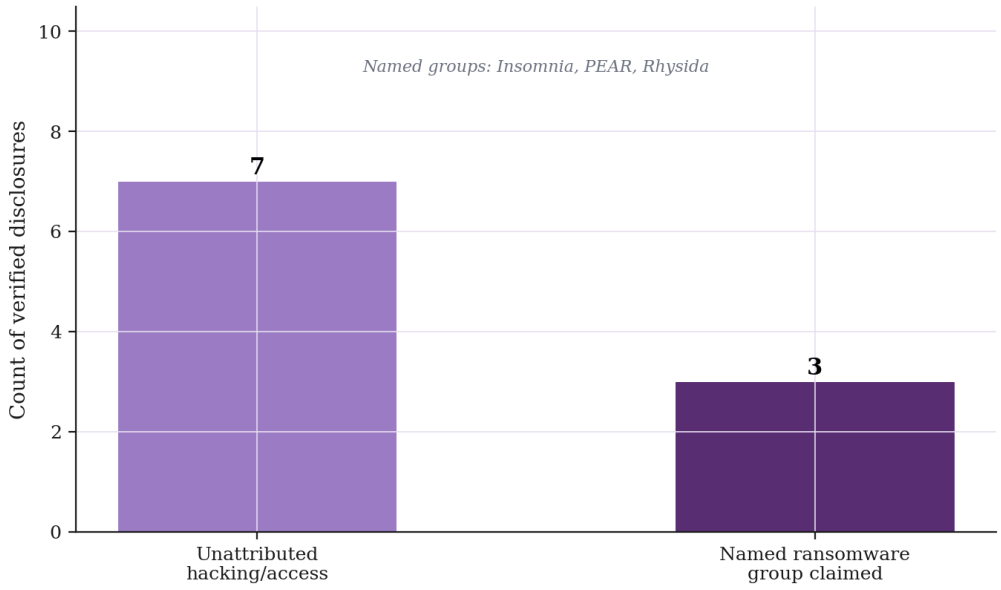

Figure 1. Vector attribution across the verified set. Seven of ten disclosures involve unattributed unauthorized access; three were claimed by named ransomware or extortion groups. Source: entity notices and independent press reporting, verified by this brief's authors.

1.4 The Specialty-Practice Long Tail

Seven of the ten verified disclosures occurred at independent specialty practices or an imaging provider — dermatology, ophthalmology, orthopedics, oncology, neurology, and radiology — rather than at the two

business-associate/AI vendors (Xsolis, Innovative Scientific Solutions) or the one hospital system (Singing River) in the verified set. This is a structural counterpoint to §1.1 and §1.2: the quarter's largest verified disclosures concentrate impact at an AI vendor and a repeat-victim imaging practice, but the volume of confirmed disclosures sits predominantly at small, independent covered entities. Both observations are true simultaneously and describe different dimensions of the same sector. Independent practices typically operate with smaller IT security budgets and staff than hospital systems or large vendors, and the pattern is consistent with the frequency dynamic the Q1 2026 report also identified: breach impact concentrates upstream, while breach frequency concentrates at the point-of-care level.

Figure 2. Verified Disclosures by Category

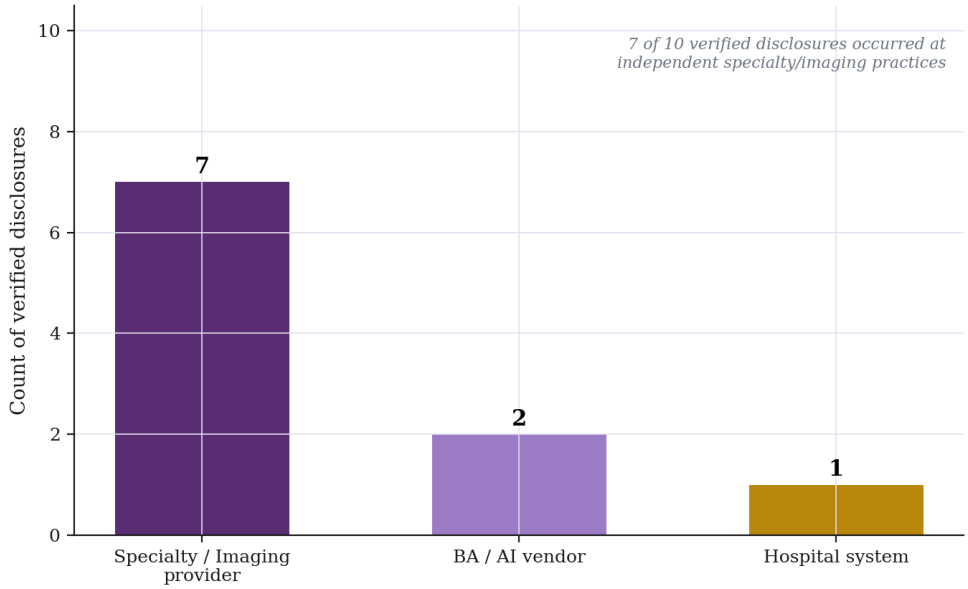

Figure 2. Verified disclosures by category. Seven of ten occurred at independent specialty or imaging providers, two at business-associate/AI vendors, and one at a hospital system. Source: entity notices and independent press reporting, verified by this brief's authors.

2. Verified Q2 2026 Breach Disclosures

The following ten incidents were individually verified against the HHS OCR breach portal and independent public reporting, with OCR submission dates confirmed within the Q2 2026 window. This is not a complete inventory of the quarter; it is the set of incidents whose Q2 OCR submission and affected count could be independently confirmed by this brief's cutoff. The Basis column states each entry's verification tier: 'A' denotes an OCR date and affected count independently confirmed through multiple concurring primary or press sources; 'B' denotes a date drawn from external portal review or a single independent source, corroborated against entity notification timing rather than multi-source convergence. Full tier definitions are in Appendix D.

Entity	Category	Affected	OCR Submitted	Basis
Xsolis, Inc.	AI / BA vendor	1,396,519	Jun 5, 2026	A

Florida Physician Specialists	Specialty provider	276,498	Apr 24, 2026	B
Radiology Associates of Richmond	Imaging provider	266,183	~May 21, 2026	A
Southern Illinois Dermatology	Specialty provider	160,312	Apr 2, 2026	B
Laurel Eye Clinic	Specialty provider	145,221	Apr 22, 2026	B
Innovative Scientific Solutions	BA vendor	143,842	Apr 17, 2026	B
Western Orthopaedics, P.C.	Specialty provider	113,330	~Apr 29–May 5, 2026	B
Minnesota Epilepsy Group, P.A.	Specialty provider	80,061	~Jun 5, 2026	A
Hematology Oncology Consultants	Specialty provider	62,972	Apr 24, 2026	A
Singing River Health System	Hospital system	53,888	~May 19, 2026	B

Figure 3. The Verified Q2 2026 Floor — Ten Confirmed Disclosures

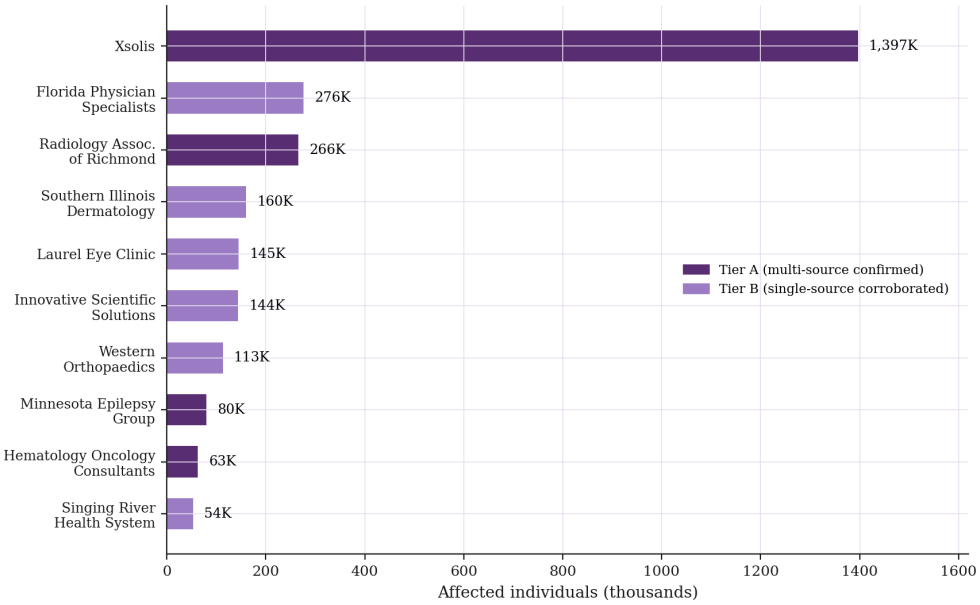

Figure 3. The verified Q2 2026 floor — ten confirmed disclosures totaling at least 2,698,826 affected individuals, colored by verification tier. Source: HHS OCR Breach Portal; entity notices; independent press reporting, verified by this brief's authors.

3. Structural Analysis: The TARF Framework in Q2

The Q1 2026 report applied the Transparency-Adjusted Risk Function (Perrin, 2025b) qualitatively, concluding that the numerator of transparency-adjusted risk was stable to rising while the denominator deteriorated. This brief extends that reading to the verified Q2 set. As in Q1, the application is qualitative: the four component indices are not re-measured numerically, and the reading rests on convergence across the incidents this brief could independently confirm rather than a full-quarter measurement.

The reusability-and-retention component, which captures how long a stolen record retains fraud value, is sharpened directly by the Xsolis disclosure (§1.1). Records belonging to a health system that ended its Xsolis relationship in 2021 were still exposed in the 2026 breach, carrying the same immutable identifiers as records generated the day before the intrusion. Retention beyond operational need is a standing contribution to this component, independent of any change in attacker behavior.

The transparency component, the sector's primary defensive lever per the Q1 framework, did not improve. Detection-to-disclosure intervals in the verified set remained long: Xsolis's interval from January attack to June OCR filing was approximately four to five months, and Radiology Associates of Richmond's first-breach interval from its April 2024 incident to its July 2025 federal filing was approximately fifteen months (§1.2). Against the finance-sector benchmark of a four-business-day disclosure rule, healthcare intervals in the verified set remained one to two orders of magnitude longer.

Synthesizing qualitatively: the Q2 verified set shows a numerator reinforced by the Xsolis retention finding, against a denominator that did not improve. This is directionally consistent with the Q1 reading of sustained sector-wide exploitability, offered as a hypothesis this series continues to track rather than an empirical demonstration.

4. Regulatory Environment

The proposed HIPAA Security Rule update, whose regulatory-agenda target for final action was May 2026, passed that window without a final rule. A coalition of more than one hundred hospital and provider groups continued to press HHS to withdraw the proposal, citing an OCR first-year compliance-cost estimate of approximately nine billion dollars. OCR continued to enforce the current Security Rule, where a missing or stale risk analysis under 45 CFR 164.308(a)(1)(ii)(A) remained the single most frequently cited deficiency; all four of OCR's April 2026 settlements involved a risk-analysis failure. For a covered entity, the practical implication is unchanged by the rule's delay: a current, documented risk analysis is both the most-cited enforcement gap under the present rule and the foundation on which every proposed change builds.

5. Recommendations

The following recommendations are derived directly from the verified Q2 2026 record in §1. They do not constitute legal advice; covered entities and business associates with specific compliance questions should consult qualified HIPAA counsel.

5.1 For Covered Entities

1. Document vendor offboarding with proof of data disposition. The Xsolis disclosure (§1.1) shows data remaining exposed years after a vendor relationship ended. When terminating a business-associate relationship, obtain and retain written confirmation of data return or destruction, not just a termination notice.

2. Treat a completed breach investigation as the start of a remediation review, not the end of the incident. Radiology Associates of Richmond's second breach (§1.2) began within weeks of its first breach's federal reporting, raising the question of whether remediation had fully taken hold. A closed investigation should trigger a documented check of whether the access vector that caused it was actually closed, not merely disclosed.

3. Maintain a current, documented risk analysis independent of Security Rule finalization timing. All four of OCR's April 2026 settlements cited a risk-analysis failure (§4); it remains the most consistently cited enforcement gap and the one most directly within an entity's control.

4. Independent and specialty practices should assume they are a primary target, not a low-priority one. Seven of the ten verified Q2 disclosures occurred at practices of this size (§1.4); attacker targeting does not track organizational size the way security budgets often do.

5. Where a named extortion group claims responsibility without encryption, as PEAR did at Western Orthopaedics (§1.3), treat the claim as an immediate exposure event rather than a ransom negotiation — the data is already circulating.

5.2 For Business Associates and Vendors

1. Publish a data-retention and disposition schedule that clients can audit. The Xsolis case is, in part, a documentation failure: whatever the vendor's internal retention practice was, no client-facing record confirmed disposition after the 2021 termination.

2. AI-enabled platforms that aggregate clinical data across many client organizations should treat that aggregation as the primary attack surface, not a byproduct of the product. The upstream-concentration pattern this series has now tracked across two quarters runs increasingly through platforms built this way.

6. Conclusion and Q3 Outlook

Two structural patterns from Q1 2026 persisted into Q2. Breach impact continues to concentrate upstream — this quarter through an AI-enabled vendor rather than a claims-processing cascade — and detection-to-disclosure intervals across named incidents remain far longer than the finance-sector benchmark (§3). A third pattern is specific to Q2's verified set: repeat-victim governance failure, illustrated by Radiology Associates of Richmond, is a risk distinct from data aggregation and merits its own tracking discipline. For covered entities and business associates, §5 translates these findings into concrete controls: vendor-offboarding documentation, post-investigation remediation review, and continued risk-analysis discipline independent of the Security Rule's finalization timeline.

Separately, this brief reports ten verified disclosures rather than a full quarter total, and that choice is itself a documented finding — detailed in the appendices — about the state of multi-source breach compilation as of this cutoff, not a gap in effort. The next volume in this series will cover Q3 2026 and is scheduled for October 2026 publication. Whether the AI-vendor aggregation pattern observed at Xsolis persists into a third quarter, and whether the underlying compilation gains the reliable date and count fields needed to support a full

quantitative review again, are the two open questions this series will track next.

Appendix A. Data Cutoff and Point-in-Time Notice

This analysis was compiled on July 2, 2026, and reflects the state of the underlying sources as of that date. The HHS OCR breach portal is not a static record of a closed quarter: it adds entries on a rolling, frequently delayed basis, and the late-2025 federal shutdown compounded the backlog, so breaches with Q2 reporting obligations were still being added after this brief's cutoff. Figures here are a point-in-time reading, not a final quarter tally; a portal query run later will show entries that did not exist on July 2. This reflects a deliberate choice of timeliness over completeness — waiting for the portal to fully settle would delay publication by months, past the point where the brief's operational value to covered entities remains current. A verified incident does not become unverified when the portal grows; this brief's claims are bounded by what could be confirmed as of the cutoff and are stable against later additions rather than contradicted by them.

Appendix B. Methodology: Source Reconciliation and Verification Standard

This compilation draws on HHS OCR, state attorney general filings, FTC records, CISA advisories, and press reporting rather than the OCR portal alone. Multi-source compilation surfaces incidents before they reach the OCR portal, captures affected-population revisions a single snapshot would miss, and enables the cross-checking against entity notices and independent press reporting by which every incident in §2 was confirmed. It also carries a reconciliation cost that single-source analysis does not face: different sources record different dates for the same incident — incident date, discovery date, state-filing date, OCR-submission date — under what a raw compilation flattens into a single timestamp field, and affected counts evolve as investigations conclude. This appendix documents that reconciliation.

The raw Q2 compilation, before verification, totaled approximately 291.7 million affected individuals across OCR and state attorney general filings. The large majority traced to three identifiable mechanisms, itemized in full in Appendix C. First, prior-year incidents re-filed at the state level: the 2015 Anthem breach (78.8 million, under multiple state settlement filings), the 2024 Kaiser Permanente tracking-technology breach (13.4 million), the 2015 Excellus breach (10.5 million), the 2023 MCNA Dental breach (8.9 million), the 2023 Harvard Pilgrim ransomware attack (2.5 million), the 2022 Professional Finance Company ransomware attack (1.9 million), the 2015 CareFirst breach (1.1 million), and a cluster of 2023 MOVEit-event notifications. Second, genuine 2026 incidents whose original OCR submission fell before April: NYC Health and Hospitals (1.8 million, OCR March 24), Navia (2.15 million, March 18), OpenLoop (716,000, March 17), Erie Family Health (570,000, March 27), and Nacogdoches (March, which also carried a digit-shift error inflating 257,073 to 2.5 million). Third, an affected-count data error: the L.A. Care figure appeared at 2,000,000 against an entity-confirmed count under 3,000, per the entity's own notice.

CONTAMINATION CONCENTRATES BY CHANNEL

HHS OCR submission dates are generally more reliable than state AG observation dates, but not sufficient alone; several state attorney general portals batch-released historical settlements and MOVEit-era re-filings with current dates, while some OCR entries appeared to reflect later revisions rather than original submission timing. Incident-date verification against primary reporting was therefore required throughout.

One further pattern is worth stating for future compilations: OCR filing dates themselves can reflect a revision rather than an original submission. Saint Anthony Hospital illustrates this directly — its incident dates to February 2025, its original OCR report was filed in September 2025 at 6,679 affected, and a 2026 data-review revision raised the figure to 146,108. Incident timing throughout this brief was therefore verified against entity notices and independent press reporting, not portal dates alone. A related case, Stockton Cardiology Medical Group, was checked and excluded on the same basis: its GENESIS ransomware incident was discovered in January 2026 and disclosed to the California Attorney General on March 9, 2026 — a Q1-origin case already documented in the series' inaugural issue, not a Q2 disclosure, despite carrying a Q2-shaped observation date in the raw export.

Appendix C. Reclassified and Excluded Incidents

In the interest of full transparency, the following incidents were removed from or held back from the verified Q2 set after checking. Saint Anthony Hospital (146,108) was originally OCR-reported in September 2025 at 6,679 affected before a 2026 upward revision, as described in Appendix B. Wound Technology Network (139,830) was detected in December 2025 with a March 2026 notice; its Q2 OCR submission could not be confirmed. Stockton Cardiology Medical Group is excluded as a Q1-origin case already covered in the inaugural issue. Each is a real incident; none met the brief's verification standard as an original Q2 2026 disclosure.

Incident	Affected	Reason Excluded
Saint Anthony Hospital	146,108	Incident Feb 2025; OCR original Sep 2025 (revised 2026)
Wound Technology Network	139,830	Detected Dec 2025; Q2 OCR submission unconfirmed
Stockton Cardiology Medical Group	N/A (Q1 case)	Q1-origin (GENESIS); CA AG filed Mar 9, 2026 — pre-Q2
Anthem, Inc.	78,800,000	2015 breach; state settlement re-filing
Kaiser Permanente	13,400,000	2024 tracking-tech; HHS filed Apr 2024
Excellus / MCNA / Harvard Pilgrim	21,900,000	2015 / 2023 re-filings
Professional Finance / CareFirst	3,018,941	2022 / 2015 re-filings

MOVEit cluster (WI filings)	~1,500,000	2023 MOVEit event re-filings
NYC H+H / Navia / OpenLoop / Erie	~5,237,000	Genuine 2026, OCR-submitted Jan-Mar (H1)
L.A. Care Health Plan	2,000,000 corrected to 2,885	Raw count error; Jan 2026 mailing error, <3,000
Nacogdoches Memorial	2,507,073 corrected to 257,073	Digit-shift error + H1 OCR submission (March)

Appendix D. Verification Tiers and Limitations

Tier definitions: 'A' denotes an entry whose OCR date and affected count were independently confirmed by this brief's authors through multiple concurring primary or press sources. 'B' denotes an entry corroborated against entity notification timing or a single independent source, rather than multi-source convergence on the exact date. Four of the ten verified entries are Tier A (Xsolis, Radiology Associates of Richmond, Minnesota Epilepsy Group, and Hematology Oncology Consultants); six are Tier B. Florida Physician Specialists' affected count is independently corroborated, but its OCR-date verification remains Tier B under this brief's standard, and the Basis column reflects that classification. This distinction is stated explicitly rather than presenting all ten entries as uniformly verified, and readers requiring the canonical OCR date for a specific entry should consult the live HHS OCR breach portal directly.

This brief is subject to further limitations a rigorous reading should weigh explicitly. It is a point-in-time compilation, not a closed-quarter record, per Appendix A. The ten verified disclosures in §2 are not a complete inventory of Q2 2026 healthcare breach activity — they are the subset whose Q2 OCR submission and affected-population figure could be independently confirmed by the cutoff date. Affected-population figures throughout are as self-reported by the breached entity and have not been independently audited by this brief's authors; such figures are commonly revised upward as investigations conclude. Attack-vector and root-cause characterizations reflect the breached entity's own disclosure or contemporaneous press reporting rather than independent forensic confirmation. Finally, the exclusion and reclassification determinations in Appendices B–C involve judgment at the margin in specific cases — Wound Technology Network, for example, where the entity's own notice does not by itself establish a confirmed Q2 OCR submission date; readers who reach a different judgment are encouraged to consult the cited primary sources directly.

References

Perrin, A. (2026a). State of Compliance: Q1 2026 Healthcare Breach Review. Vol. 1, Issue 1. Secure Care Research Institute, Patient Protect LLC. https://patient-protect.com/research/state-of-compliance-q1-2026

HHS Office for Civil Rights. (2026). Breach portal: Notice to the secretary of HHS breach of unsecured protected health information. U.S. Department of Health and Human Services. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (accessed July 2, 2026).

SecurityWeek. (2026). Coverage of healthcare breach disclosures, including Radiology Associates of Richmond and related incidents. SecurityWeek.

DataBreaches.net. (2026). Radiology Associates of Richmond discloses second data breach; 266k people affected.

TechTarget / HealthITSecurity. (2026). First-half 2026 healthcare breach compilation and OCR portal analysis.

Entity breach notices. (2026). Direct notices published by Xsolis, Inc.; L.A. Care Health Plan; NYC Health and Hospitals Corporation; Saint Anthony Hospital; Radiology Associates of Richmond; Minnesota Epilepsy Group; and Singing River Health System.

Perrin, A. (2025b). The cyber-economic stack. Secure Care Research Institute, Patient Protect LLC. SSRN Working Paper 5792382.

Independence, Citation, and Correction Policy

This brief is produced by the Secure Care Research Institute, an independent research program operating under Patient Protect LLC. It does not rank, evaluate, or endorse any compliance software or consulting vendor, including Patient Protect's own products, and it does not constitute legal advice. Readers with compliance questions specific to their organization should consult qualified HIPAA counsel.

Suggested citation: Perrin, A. (2026b). Q2 2026 Verified Breach Brief. The State of Compliance Series, Vol. 1, Issue 2 (Brief). Secure Care Research Institute, Patient Protect LLC.

This is Version 1.0 of this brief, published July 2026 from sources current as of the July 2, 2026 cutoff stated throughout. Given the OCR portal's ongoing revisions, a reader who identifies a figure in this brief materially superseded by subsequent primary-source disclosure is invited to contact info@patient-protect.com; substantiated corrections will be published as a dated erratum appended to this issue rather than as a silent edit to the original text.