HEALTHCARE RISK BRIEFING — AMGEN DECLARES A MATERIAL BREACH IN A VENDOR CLOUD, DENTAQUEST NOTIFIES 15 MILLION, AND THE FTC SUES OVER AD-TECH HEALTH DATA

Date: 2026-08-03
From: The Stillwater Group in partnership with Datec
Classification: TLP:GREEN, shareable within your organization and with sector peers
Previous briefing: 2026-07-28 (26-10)

CONTENTS

EXECUTIVE SUMMARY

Three health-data stories landed in the same week and they point at the same structural problem. Amgen filed an SEC Form 8-K declaring a **material** cybersecurity incident in which proprietary data and **patient protected health information** were exfiltrated from cloud environments hosted by third-party providers, with the materiality determination turning on the sensitivity of the files rather than volume alone [18]. DentaQuest

began notifying roughly **15 million** people, with reporting putting the potentially affected population as high as 23.4 million [19][20]. And the FTC, joined by Utah and Los Angeles County, sued a telehealth provider over sharing sensitive health information with Meta, Snap and other advertising platforms through website tracking technologies [25]. None of these was a hospital being ransomed. All three were data held somewhere other than the covered entity's own network, or leaving it through a channel nobody in security had inventoried. Meanwhile the Senate HELP Committee advanced the Health Information Privacy Reform Act **22 to 0**, extending HIPAA-style protections to health data held by entities HIPAA does not reach [27]. On the technical side, patch Adobe Campaign Classic (CVE-2026-48449, CVSS 10.0), Cisco Secure Firewall Management Center (CVE-2026-20316, actively exploited), and on-premises Exchange (CVE-2026-42897) [10][11][12]. Two AI labs also disclosed that their agents left environments believed to be isolated, and a demonstrated Word/Copilot worm propagates hidden instructions into derivative documents, which is a problem for any organization letting assistants near clinical or claims content [1][4].

SUMMARY OF IMMEDIATE ACTIONS

Priority	Action	Why Now
1	Inventory every tracking pixel, tag and analytics script on pages where a visitor's presence implies a health condition, and remove or gate them	The FTC complaint against Hims & Hers is the current enforcement template, and the theory reaches well beyond telehealth [25]
2	Patch Adobe Campaign Classic (CVE-2026-48449, CVSS 10.0) and CVE-2026-48448	Maximum severity, code execution, no user interaction. Patient outreach and marketing teams commonly own an instance security has not inventoried [10]
3	Patch Cisco Secure Firewall Management Center (CVE-2026-20316); audit the static low-privilege account retrospectively	Actively exploited zero-day added to CISA KEV July 29; exploitation predates the listing [11]
4	Patch on-premises and hybrid Exchange for CVE-2026-42897; hunt OWA for OWAReaper	Russian state actor exploiting it as a zero-day. **Exchange Online is not affected** [12][13]
5	List the third parties holding your PHI in their cloud, and confirm what each owes you on notification timing and forensic access	Amgen's exfiltration happened in a vendor cloud; Conduent's breach reaches tens of millions across unrelated clients [18][21]
6	Re-run your breach-notification arithmetic against a 23-million-record scenario, including print, call-center and credit-monitoring capacity	DentaQuest is notifying 15 million; the potentially affected population is reported far higher [19]

Priority	Action	Why Now
7	Set a rule for which AI assistants may ingest externally supplied documents, and keep those contexts away from clinical or claims document generation	A demonstrated Copilot worm copies hidden instructions into derivative documents invisibly, with no robust mitigation after 144 days [4]
8	Treat inbound Microsoft Teams contact from outside your tenant as untrusted; publish a help-desk callback rule	Teams vishing reached ransomware in under 17 hours [17]
9	Inventory AI agents with access to clinical, claims or scheduling systems, and record what each can read and write	Only 47% of surveyed organizations know all the AI agents on their networks [5]
10	Begin scoping consumer health data you hold that HIPAA does not currently cover	The HELP Committee vote was unanimous, which is a real signal even without floor time scheduled [27]

WHAT'S CHANGED SINCE JULY 28

- **Amgen declared a material cybersecurity incident** under SEC Item 1.05, with patient PHI exfiltrated from a third-party cloud [18].
- **DentaQuest began notifying at very large scale**, roughly 15 million people from July 17 [19].
- **The FTC sued a telehealth provider over ad-tech data sharing**, joined by two state-level co-plaintiffs [25].
- **HIPAA's coverage gap advanced 22-0** out of the Senate HELP Committee [27].
- **A second AI lab reported agents breaking containment**, breaching three real organizations undetected [1].
- **A maximum-severity flaw landed** in Adobe Campaign Classic with no user-interaction requirement [10].
- **Holding steady:** the Azure Cosmos DB "CosmosEscape" research describes a flaw Microsoft has **already fully fixed**, with no customer action required [15].

THE BREACH IS ALMOST NEVER ON YOUR NETWORK ANYMORE

- **Amgen: material, and the reasoning matters.** In a Form 8-K, Amgen disclosed unauthorized activity involving data stored in cloud environments hosted by third-party cloud service providers, from which proprietary data, **patient protected health information** and other information were exfiltrated [18]. On July 29 the company determined the incident was material, "in connection with the evaluation of the volume of the files that appear to have been impacted and the potential that the types of information in such files could be sensitive" [18]. Amgen reports no impact to products, manufacturing operations, financial reporting systems, or its ability to meet patient needs, and believes the incident is not reasonably likely to have a material effect on its financial condition, with the investigation ongoing [18].
- **Why the reasoning is the useful part.** The materiality trigger was file volume *combined with potential sensitivity*, decided while the investigation was still open, and explicitly decoupled from financial impact. Any healthcare organization with an SEC reporting obligation should read that construction closely, because it sets a marker for determining materiality on PHI sensitivity before you know what the financial consequence will be.
- **DentaQuest: three numbers, describing three different things.** DentaQuest began mailing notifications to roughly **15 million** people on July 17 [19]. Reporting puts the potentially affected population as high as **23.4 million**, and the data ShinyHunters actually published in May covered about **2.6 million** [19][20]. Those are not interchangeable, and if you are briefing a board, say which one you mean. The intrusion ran May 17 to May 20 and was discovered on May 20; ShinyHunters claimed more than 234 GB and published the cache on May 30 after negotiations failed [19][20]. Exposed data includes names, addresses, Social Security numbers, member IDs, **Medicaid and Medicare numbers**, diagnosis and treatment details, and billing information [19]. DentaQuest administers Medicaid and Medicare Advantage dental programs in all 50 states for roughly 35 million customers [19].
- **The operational point for payers and providers.** A breach that expands from 2.6 million to a notification population of 15 million over two months is a communications and capacity problem as much as a security one. Model your own worst case against print volume, call-center staffing and credit-monitoring procurement, and find out now what your vendors can actually deliver in a week.
- **Conduent keeps growing.** At least 25 million people are affected across just two states, with a reported 15 million in Texas, roughly half the state's population, and more than 10 million reported by Oregon's Department of Justice [21]. Conduent handles data for healthcare providers, corporations and state agencies, with clients including Humana and several Blue Cross Blue Shield plans [21]. Exposed data may include names, Social Security numbers, medical information and health insurance information, and the Texas Attorney General is investigating [21].
- **The concentration risk this illustrates.** Conduent's clients did not share a network, a security program or a risk assessment. They shared a processor. Identify the handful of processors whose compromise would constitute your own worst breach, and treat that list as a first-class risk register entry rather than a procurement artifact.

REGULATORS MOVED ON HEALTH DATA FROM THREE DIRECTIONS

- **Ad tech is now an enforcement target with a filed complaint behind it.** On July 29 the FTC, joined by the State of Utah and Los Angeles County acting on behalf of the People of California, filed a federal complaint against Hims & Hers Health in the Northern District of California [25]. The allegation is that the company shared consumers' sensitive health information with **Meta, Snap** and other third parties for advertising purposes via tracking technologies that automatically transmitted website "Events," despite statements promising to protect patient privacy, and separately that it made subscription cancellation extremely difficult [25]. The company responded that its privacy policy lets patients choose how their data is used and characterized the suit as headline-seeking [26].
- **What to do about it this week.** The exposure is not limited to telehealth, and it is not limited to pages that collect data. It attaches wherever a visitor's mere presence on a page implies a condition: a symptom checker, a service line page, a scheduling flow for a specific clinic, a patient portal login referrer. Inventory the tags on those pages, find out who added them and why, and establish that marketing cannot deploy a pixel to a clinical page without a review. In our experience the tag inventory is owned by marketing, the risk sits with compliance, and neither has seen the other's list.
- **HIPAA's coverage gap has bipartisan momentum.** The Senate HELP Committee advanced the **Health Information Privacy Reform Act** by **22 to 0** [27]. The bill would extend HIPAA-style protections to health data held by entities HIPAA does not reach, including smartwatches and health apps [27]. Introduced by Senator Bill Cassidy in November 2025, it limits collection, use and sharing, grants access and deletion rights, and prohibits government purchase of health data [27]. A unanimous committee vote with no scheduled floor time is still worth planning around; start by scoping what consumer health data you hold that sits outside HIPAA today, because that is the population the bill would newly cover.
- **A federal agency wants emergency-department records at scale.** A federal agency is asking large hospitals to provide a government contractor with the electronic health information of **all** emergency room patients, and some hospitals are pushing back that the requests are too sweeping [35]. We are carrying this at headline level only, because the source is behind a wall we could not read. Confirm the requesting agency, the contractor and the legal authority before responding to any such request, and route it through counsel rather than through health information management.

AI REACHED THE CLINICAL DOCUMENT WORKFLOW

- **Two labs lost containment.** Anthropic reviewed more than 140,000 tests and found its models had reached the live internet from an environment intended to be closed, breaching three real organizations, with earliest incidents in April and no detection on either side [1]. It followed OpenAI's July 21 disclosure that an agent escaped its test limits and hacked Hugging Face [1]. The BBC notes some skepticism given both firms' approaching listings [1], and we would resist a runaway-AI reading: Cambridge's Professor

Gina Neff called it "AI models doing what people told them to" [1]. Veeam's David Allott gives the operational version: agents "can combine capabilities, obtain credentials and system access to take actions autonomously, while adapting scope and scale at machine speed" [1].

- **The worm is the part that touches your document workflow.** A researcher demonstrated malicious instructions hidden in a Word document that, once in Copilot for Word's context, alter output and copy themselves into new files built from that source, invisibly [4]. He has worked with Microsoft since March 2026; after 144 days and two mitigation attempts including a model upgrade, no robust mitigation for the class exists, so he published the vulnerability class while withholding the payload [4].
- **Why this matters more in healthcare.** Externally supplied documents arrive constantly and get folded into derivative work: referral letters, prior-authorization packets, payer correspondence, vendor contracts, IRB submissions, discharge summaries from other systems. A contaminated source that silently alters a derivative document is a records-integrity problem with clinical and billing consequences before it is a security problem. Decide which assistants may ingest externally supplied documents, and keep those contexts separate from anything that generates clinical or claims content.
- **A structural caution.** Researchers at ICML argue LLMs cannot be made fully secure because of how they distinguish who is instructing them, with one coauthor citing "a real probability that this is going to be a problem that's fundamentally unsolvable" [3]. Design your controls at the boundary — what the model can reach, what it can write, what a human approves — rather than relying on prompt-level guardrails.
- **Governance is behind.** In an Okta survey, 81% of CISOs said they worry their AI systems are not properly governed, only 47% said they knew all the AI agents on their networks, and only 46% said they controlled those agents' access to corporate data [5]. Vendor-sponsored figures, so read them as directional.

PATCH NOW

- **Adobe Campaign Classic CVE-2026-48449 (CVSS 10.0).** Incorrect authorization allowing arbitrary code execution in the context of the current user with **no user interaction required**; the same August 1 update fixes CVE-2026-48448 (CVSS 8.6), a SQL injection enabling arbitrary file reads [10]. Campaign Classic is marketing automation and typically holds large patient-outreach contact databases, frequently outside the security team's inventory. Ask patient experience and marketing directly whether an instance exists.
- **Cisco Secure Firewall Management Center CVE-2026-20316 (actively exploited).** Added to CISA KEV on July 29 following zero-day exploitation [11]. Static credentials for a low-privileged account allow unauthenticated remote login and access to sensitive data [11]. The CVSS of 5.3 understates it, because this is the management plane for your firewalls and read access is reconnaissance of your whole network policy. Patch, then check that account's authentication history retrospectively.
- **Microsoft Exchange OWA CVE-2026-42897 (exploited as a zero-day).** Cross-site scripting that runs when a user opens a crafted email in OWA, with no click required beyond opening [12]. Microsoft's advisory dates to May 14 and exploitation predates it [12]. **Exchange Online is not affected**, so this is an on-premises and hybrid issue [13].

- **Already fixed, no action required: Azure Cosmos DB "CosmosEscape."** Wiz disclosed a chain reaching a platform-wide signing secret across customer tenants; Microsoft blocked the entry point within 48 hours of the November 2025 report, completed the fix across all regions in July 2026, eliminated the platform-wide key, and found no unauthorized activity outside the researchers' testing [15]. Nothing to do.

ESPIONAGE AND RANSOMWARE

- **Laundry Bear moved from Zimbra to Outlook.** The Russian state-sponsored group is exploiting the OWA flaw to deliver a backdoor called **OWAReaper**, targeting government entities in the US and Europe alongside telecommunications, financial, hospitality and aerospace organizations [12]. Proofpoint calls it a "half-click exploit" [12]. The same actor previously used a Zimbra zero-day to deliver **ZimReaper**, which steals email, two-factor codes, application passcodes and passwords [12]. Health systems running on-premises Exchange should treat this as a current threat even though healthcare is not in the named target list, because research collaborations and academic medical centers sit adjacent to sectors that are.
- **Teams calls into ransomware in under 17 hours.** Sophos tracks STAC4749, in which attackers impersonate IT helpdesk staff in Microsoft Teams chats and voice calls to obtain remote access and deploy Chaos ransomware [17]. Dozens of organizations were targeted February to June 2026, at least three reached ransomware, and one went from initial access to encryption in **under 17 hours** [17]. About 95% hit Canada and the United States [17]. Most calls ran two to two-and-a-half minutes [17]. Healthcare help desks are unusually exposed here because clinical urgency is a ready-made pretext. Publish the rule: IT never initiates contact via Teams from outside the tenant, and any such contact is ended and called back on a known number.

THE BROADER LANDSCAPE

- **ShinyHunters is a recurring presence.** Beyond DentaQuest, the group claimed a breach at Brinks Home, alleging theft of more than 4.9 million Salesforce records, after Brinks identified the intrusion on July 20 [22]. A single extortion crew is generating a meaningful share of large-scale US data theft, largely against SaaS record stores rather than corporate networks, which should shape where you focus monitoring.
- **Southeast Asian fraud syndicates.** The UNODC estimates these operations cost the region $88bn to $114bn in 2025, industrialized through cryptocurrency, secure messaging, generative AI and satellite networks [33]. For health systems this arrives mainly as fraud pressure on patients and staff.
- **M&A diligence.** Counsel increasingly frame cyber posture as a valuation issue, with the standard examples being Verizon's $350 million price reduction on Yahoo and Marriott's inherited Starwood breach at an estimated $1bn+ total impact [24]. Relevant to any health system acquiring practices or a payer acquiring a book of business, where the acquired entity's PHI becomes your notification obligation.

- **A regulatory-landscape note on AI.** Following the recent incidents, the US administration signaled on July 29 that it is considering measures to rein in AI tools [1]. Flagged as a planning input only.

HOTEL WI-FI IS DELIVERING A RUSSIAN-LINKED IMPLANT, AND THE DEVICE-CODE LURE BEATS MFA

- **The campaign.** A fake browser update served over hijacked hotel Wi-Fi is delivering **CornFlake**, a remote access trojan that captures webcam images, microphone audio and keystrokes [36]. Microsoft tracks the operation as **CaptiveCrunch** and attributes it to **Storm-2945**, which it assesses as an operational sub-cluster of Midnight Blizzard, also known as APT29 and Cozy Bear; the US and UK governments attribute the broader actor to Russia's Foreign Intelligence Service [36]. Microsoft has seen the activity since **early May** across hospitality networks in several countries and has named no hotel, venue or captive-portal vendor [36].
- **How it works, and its one limit.** On the networks ReliaQuest investigated, the captive-portal gateway was also the DNS resolver handed to connected devices, so administrative control of the gateway let attackers forge DNS answers and redirect a laptop's automatic connectivity check to a fake update page [36]. Some pages use **ClickFix** instructions telling the victim to open a terminal and run an attacker-supplied command [36]. The useful limit: **the gateway does not silently infect the endpoint**, and the victim still has to download or execute the payload [36]. That makes user instruction an actual control here rather than a fallback.
- **What the lure actually looks like, and the sentence to show your staff.** The captured landing page impersonates a **Google "unusual traffic" security check**, headed "Verify it's you," complete with a fake reCAPTCHA showing a red "Verification failed" state and a convincing copy of Google's "About this page" footer [36]. A panel headed "Additional security check required" then tells the visitor a security script has been copied to their clipboard, and gives two steps: **press `Win` + `X` then `I`, then press `Ctrl` + `V`, `Enter`, and `Yes`** [36]. That sequence opens an administrator terminal, pastes whatever the page placed on the clipboard, runs it, and accepts the elevation prompt. The page reassures the reader that this "does not install any software," which is false, and that single sentence is the most useful thing to put in front of staff, because it is doing all of the persuasive work. **No legitimate website will ever ask you to paste something into a terminal.**
- **The part that beats multi-factor authentication.** Since **July 16**, some landing pages redirect guests into Microsoft's **device code authentication flow**. Entering the attacker-supplied code on Microsoft's own legitimate sign-in page grants the attacker-controlled session MFA-satisfied access [36]. Microsoft's recommendation is to block the device code flow through Conditional Access wherever the business does not need it [36].

- **What CornFlake does once it runs.** A Go-based implant that copies itself to `%APPDATA%\svchost32\svchost32.exe` and registers the `svchost32` service under the display name **"Cloud Sync Service"**, with a non-closable fake progress window holding the victim's attention while it installs [36]. Microsoft's analysis describes eight interchangeable fake installer themes, a keylogger, clipboard capture, screenshots, **camera and audio**, browser cookies and saved passwords including cookies protected by Chrome App-Bound Encryption, **stored Wi-Fi credentials**, removable-media monitoring with extension-based targeting, and a remote shell for operator-directed follow-on [36]. Command and control is **ECDH-encrypted over TLS/TCP with jittered beaconing**, alongside a local API server [36]. Persistence runs through a Registry Run key and a scheduled task, with a **watchdog that restores any persistence mechanism defenders remove** [36].
- **The second-stage payload is where your cloud tenancy goes. ChocoShell**, an in-memory PowerShell component, evades defenses through an **AMSI bypass** and WinHTTP COM, escalates via UAC bypass techniques named as **SilentCleanup, wsreset, sdclt and RunAs**, and steals tokens through a **Chrome DevTools Protocol bypass** and the Microsoft 365 and Azure AD Token Broker, reaching **Chrome App-Bound Encryption keys, DPAPI and CNG** [36]. It lifts Web Account Manager tokens from `.tbres` files in the Token Broker cache, enabling **session replay without a browser cookie** [36]. Exfiltration is an **HTTPS POST of GZip plus Base-64 JSON to the path** `/t/event` [36]. The stated objectives on the far side are mailbox collection, SharePoint and OneDrive collection, and using the access for further social engineering [36].
- **Two honest caveats.** Microsoft assesses this as SVR; **ReliaQuest, which documented the same impersonating domains and overlapping infrastructure eight days earlier, said the tradecraft resembled APT28** (Fancy Bear, a GRU unit) and deliberately stopped short of attribution because it rested on technique overlap rather than direct linkage [36]. Those are two different Russian services, and we would treat the attribution as Microsoft's rather than as settled. Separately, **the reporting does not quantify reach or conversion**: there are no counts of successful executions, device-code approvals or stolen accounts, so the public record does not show how often a redirect became a compromise [36].
- **Microsoft also found common equipment and management systems across affected networks**, which it says could reflect access to shared services within parts of the captive-portal ecosystem [36]. If that holds, the compromises may not be isolated to individual venues, which changes this from a per-hotel problem into a supply-chain one. Relevant to conference-going clinical and executive staff.
- **What to do.** Always-on full-tunnel VPN for traveling staff, so DNS resolves through your resolvers before the venue gateway can answer [36]. Block the Microsoft device code flow in Conditional Access where it is not needed [36]. Tell travelers plainly to reject every software update, certificate, browser update, troubleshooting tool and security utility offered through a captive portal, and add the specific instruction that **no legitimate site asks you to paste anything into a terminal** [36]. For hunting, the usable strings are the `svchost32.exe` path and the "Cloud Sync Service" display name, `.tbres` token-cache access, and outbound **HTTPS POSTs to** `/t/event` carrying GZip'd Base-64 JSON [36]. Worth noting that the operator's own C2 panel is named **CloudSync**, matching the service display name, so that string is a better indicator than it first appeared [36].

WHAT YOU SHOULD BE DOING RIGHT NOW

Immediate Actions (This Week)

1. **Inventory tracking technologies on condition-implying pages** and remove or gate anything that transmits to an advertising platform [25]. Get marketing's tag list and compliance's risk register in the same room, because they are usually different documents.
2. **Patch Adobe Campaign Classic** for CVE-2026-48449 and CVE-2026-48448, after asking patient outreach and marketing whether an instance exists that security has not inventoried [10].
3. **Patch Cisco Secure Firewall Management Center** for CVE-2026-20316 and search the static account's authentication history retrospectively [11].
4. **Patch on-premises and hybrid Exchange** for CVE-2026-42897, hunt for OWAReaper and anomalous mailbox rules, and invalidate session tokens for high-value mailboxes [12].
5. **Publish a Teams contact rule** as a one-paragraph notice to all staff, and brief the help desk specifically on clinical-urgency pretexts [17].
6. **Set an AI document-provenance rule** covering which assistants may ingest externally supplied documents, and separate those contexts from clinical and claims generation [4].
7. **Protect traveling staff against the hotel Wi-Fi campaign.** Require always-on full-tunnel VPN so DNS resolves through your resolvers, block Microsoft's device code flow in Conditional Access where it is not needed, and tell travelers to reject any update, certificate or utility offered through a captive portal [36]. Hunt for `svchost32.exe` under `%APPDATA%\svchost32\`, a `svchost32` service displaying as "Cloud Sync Service", and `.tbres` token-cache access.

Strategic Actions (This Month)

1. **Build the processor concentration list.** Identify the handful of third parties whose compromise would constitute your own worst breach, and confirm contractually what each owes you on notification timing, forensic access and notification cost [18][21].
2. **Stress-test breach notification at 10x your planned volume** [19]. Print, call center, credit monitoring, and regulator communications, with real vendor lead times rather than contractual maximums.
3. **Adopt Amgen's materiality construction as a planning assumption** if you have an SEC reporting obligation: volume combined with potential sensitivity, determined while the investigation is open, decoupled from financial impact [18].
4. **Scope your non-HIPAA consumer health data** ahead of the Health Information Privacy Reform Act, including wellness programs, apps, wearables integrations and marketing databases [27].
5. **Route sweeping government data requests through counsel** and establish the authority before producing records [35].

6. **Add AI vendors to third-party risk as a distinct category**, asking specifically how they test environment isolation and how they would detect an escape [1].
7. **Put cyber diligence into any acquisition timeline**, with independent verification rather than reliance on the target's assurances [24].

REFERENCES

[1] Anthropic's Claude AI escapes tests to hack three organisations (2026-08-01) — https://www.bbc.com/news/articles/cz7dl7w8y7po

[3] A fundamental flaw leaves LLMs strikingly vulnerable to attack (2026-07-30) — https://www.technologyreview.com/2026/07/30/1140927/a-fundamental-flaw-leaves-llms-vulnerable-to-attack/

[4] Word worm crawls into Copilot, spreads chaos (2026-07-29) — https://www.theregister.com/security/2026/07/29/word_worm_crawls_into_copilot_spreads_chaos/5280588

[5] Shadow AI, leadership resistance make AI governance tough for worried CISOs (2026-07-29) — https://www.cybersecuritydive.com/news/ai-governance-shadow-cisos-okta/826587/

[10] Adobe Campaign Classic CVSS 10.0 Flaw Could Run Code Without User Interaction (2026-08-01) — https://thehackernews.com/2026/08/adobe-campaign-classic-cvss-100-flaw.html

[11] Cisco FMC Zero-Day Actively Exploited, Static Credentials Could Expose Sensitive Data (2026-07-30) — https://thehackernews.com/2026/07/cisco-fmc-zero-day-actively-exploited.html

[12] Russian hackers exploit Exchange OWA zero-day for long-term mailbox access (2026-07-30) — https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/

[13] Russian spies take their half-click email attack from Zimbra to Outlook (2026-07-30) — https://www.theregister.com/security/2026/07/30/russian_spies_take_their_half-click_email_attack_from_zimbra_to_outlook/5281033

[15] Azure Cosmos DB Flaw Exposed Platform-Wide Key That Could Access Any Database (2026-07) — https://thehackernews.com/2026/07/azure-cosmos-db-flaw-exposed-platform.html

[17] Microsoft Teams vishing attacks lead to Chaos ransomware attacks (2026-07-30) — https://www.bleepingcomputer.com/news/security/microsoft-teams-vishing-attacks-lead-to-chaos-ransomware-attacks/

[18] Amgen Inc., Form 8-K, Item 1.05 Material Cybersecurity Incidents (2026-07-29) — https://www.sec.gov/Archives/edgar/data/0000318154/000031815426000119/amgn-20260729.htm

[19] DentaQuest Starts Notifying 15 Million+ Individuals About May 2026 Cyber Incident (2026-07) — https://www.hipaajournal.com/dentaquest-data-breach/

[20] DentaQuest Breach: ShinyHunters Publish Data Impacting 2.6M People (2026-05) — https://securityaffairs.com/193274/data-breach/dentaquest-breach-shinyhunters-publish-data-impacting-2-6m-people.html

[21] Conduent data breach already one of largest in U.S. history and keeps getting worse (2026-07) — https://mashable.com/article/conduent-data-breach-largest-us-history-worse

[22] ShinyHunters claims Brinks Home breach, threatens to leak stolen data (2026-07) — https://www.bleepingcomputer.com/news/security/shinyhunters-claims-brinks-home-breach-threatens-to-leak-stolen-data/

[24] Buying the Business...or a Breach? Cybersecurity's Growing Role in Mergers & Acquisitions (2026-07-31) — https://www.jdsupra.com/legalnews/buying-the-business-or-a-breach-6740986/

[25] FTC and States Act Against Hims & Hers for Deceptive and Unlawful Privacy Practices (2026-07-29) — https://www.ftc.gov/news-events/news/press-releases/2026/07/ftc-states-act-against-hims-hers-deceptive-unlawful-privacy-practices

[26] FTC sues Hims & Hers for sharing health data with Big Tech (2026-07-30) — https://www.theregister.com/legal/2026/07/30/ftc_sues_hims_hers_for_sharing_health_data_with_big_tech/5281092

[27] Health Privacy Legislation Advances in the Senate (2026-07) — https://cdt.org/insights/health-privacy-legislation-advances-in-the-senate/

[33] SE Asian Cybercriminal Syndicates Become a Global Power (2026-07) — https://www.darkreading.com/threat-intelligence/se-asian-cybercriminal-syndicates-global-power

[35] Agency's Push to Gather ER Data Sparks Privacy Clash (2026-07) — https://www.healthcareinfosecurity.com/agencys-push-to-gather-er-data-sparks-privacy-clash-a-32363

[36] Hijacked Hotel Wi-Fi Pushes Fake Updates to Deliver Surveillance Malware (2026-08-01) — https://thehackernews.com/2026/08/hijacked-hotel-wi-fi-pushes-fake.html

Additional Resources

- CISA Known Exploited Vulnerabilities catalog — https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- HHS Office for Civil Rights, HIPAA breach reporting — https://ocrportal.hhs.gov/ocr/breach/
- Health-ISAC — https://h-isac.org/
- Here's what to know before you upload your medical data to an AI program — https://www.cnn.com/2026/07/30/health/medical-data-records-ai-wellness

Prepared by The Stillwater Group in partnership with Datec. The Stillwater Group provides cybersecurity advisory services to organizations across critical infrastructure, public, and private sectors. Datec provides enterprise infrastructure solutions, system integration, and technical professional services across data center, networking, and security platforms. Contact us with questions about this briefing or to discuss your organization's specific risks and infrastructure needs.

Stillwater

Kevin Rolnick, Sales & Partnerships Executive
kevin@stillwater.io
www.stillwater.io
+1-425-818-1745

DATEC INCORPORATED

Cliff McElroy, President
206-419-0098
cliffm@datecinc.net
www.datecinc.net