

FORTUNE FAVORS THE PREPARED

DAILY THREAT REPORT

BUSINESS EDITION — HEALTHCARE & HOSPITAL OPERATIONS

31 MARCH 2026

Operation Epic Fury — Day 32 | **PREP-CON 3: ELEVATED**

Coverage in This Edition:

Cyber Threat (Iranian Actors) | Legislative & Regulatory Tracker (4-Lane)
Financial Pressure (Medicaid / Reimbursement) | Workforce / Labor
Supply Chain / Medical Device | Physical Security & Operational Continuity

fortunefavorstheprepared.com

RESTRICTED DISTRIBUTION — AUTHORIZED SUBSCRIBERS ONLY

**PREP-CON
3**

ELEVATED — Active US-Israel operations against Iran (Op Epic Fury, Day 32). Iranian cyber actors have demonstrated deliberate focus on the medical sector. Stryker wiper attack confirmed (11 Mar, DOJ attribution 21 Mar). Second unnamed US healthcare provider hit with destructive ransomware (confirmed by Halcyon). OBBBA Medicaid cuts live — first provisions effective 2026.

Operational Basis: DOJ formally attributed Stryker attack to Iran MOIS (21 Mar). Halcyon confirms second healthcare sector hit. HIPAA Security Rule final rule expected May 2026. OBBBA Medicaid work requirements effective 31 Dec 2026. 340B rebate model RFI comment deadline 20 Apr. OPSS drug acquisition cost survey closes 31 Mar. Full PREP-CON: fortunefavorstheprepared.com/preparedness-book-of-knowledge-2/planning/preparedness-conditions-prep-con/

BLUF — BOTTOM LINE UP FRONT

Healthcare and hospital operators face a two-front threat environment with no modern precedent: a state-sponsored adversary demonstrably focused on the medical sector, and the most consequential federal legislative restructuring of healthcare financing since the ACA. On the operational threat side, the DOJ on 21 March formally attributed the Stryker wiper attack to Iran's MOIS — the first formal attribution of a destructive attack on US soil to Iran during the current conflict. Halcyon has confirmed a second unnamed US healthcare provider was hit with destructive ransomware using Iran-linked tooling, with no ransom demand, suggesting a deliberate destruction campaign. Cybersecurity experts are explicit: this is a deliberate focus on the medical sector, not opportunistic targeting. On the policy side, the One Big Beautiful Bill Act (OBBBA) signed 4 July 2025 set in motion the largest Medicaid funding reduction in the program's history — \$1 trillion over 10 years — with multiple provisions effective in 2026 and work requirements hitting 31 December 2026. The HIPAA Security Rule final rule is expected May 2026. The 340B rebate model RFI comment deadline is 20 April. The OPSS drug acquisition cost survey closes today, 31 March. Hospital CFOs, COOs, and CISOs are not watching these threats from different silos — they are converging on the same institutions simultaneously.

CYBER	DOJ attributed Stryker attack to MOIS (21 Mar). Second US healthcare provider hit with Iran-linked ransomware (Halcyon confirmed). Deliberate medical sector targeting pattern emerging. CISA at ~38% staffing.
MEDICAID	OBBBA: \$1T cuts over 10 years. Work requirements effective 31 Dec 2026. Enhanced FMAP sunset 1 Jan 2026 (already effective). 11.8M projected to lose coverage by 2034. Safety-net, children's, and rural hospitals most exposed.
HIPAA CYBER	Security Rule final rule expected May 2026. All 'addressable' specs become mandatory — MFA, encryption, vulnerability scanning, pen testing, 72-hr recovery. Compliance window: 180 days from publication (~Nov 2026 effective).
340B	Rebate model RFI comment deadline 20 Apr 2026. OPSS drug cost survey closes 31 Mar (TODAY). Child site court ruling (3 Mar) vacated HRSA advance registration requirement. Program in active restructuring — covered entity revenue at risk.
WORKFORCE	Near 1-in-5 nursing vacancies in rural markets. 1.1M noncitizen healthcare workers facing immigration enforcement uncertainty. Physician shortage projected 86,000 by 2036. International nurse recruitment disrupted by visa uncertainty.

SUPPLY CHAIN

Stryker systems disrupted — ordering, manufacturing, shipping affected. ECG transmission to hospitals disrupted (Maryland paramedics reported). Medical device supply chain exposed to Iranian cyber targeting and Hormuz logistics disruption.

FLASH ENTRIES — IMMEDIATE OPERATIONAL SIGNIFICANCE

⚡ FLASH — CYBER / PATIENT SAFETY | DOJ Formally Attributes Stryker Attack to Iran MOIS — Medical Sector Deliberately Targeted

On 21 March 2026, the Department of Justice formally attributed the 11 March Stryker cyberattack to Iran's Ministry of Intelligence and Security (MOIS). Handala Hack hijacked Stryker's Microsoft Intune administrator account and triggered factory resets on 200,000+ devices across 79 countries — no malware required; they used legitimate device management infrastructure as a weapon. Maryland paramedics reported loss of ECG transmission capability to hospitals as a direct patient safety consequence. Simultaneously, Halcyon confirmed a second unnamed US healthcare company was hit with Iranian-linked destructive ransomware — no ransom demanded, suggesting deliberate destruction, not financial motivation. Cynthia Kaiser (Halcyon SVP): 'This suggests a deliberate focus on the medical sector rather than targets of opportunity. As this conflict continues, we should expect that targeting to intensify.' Hospital CISOs should treat this as active, not precautionary.

⚡ FLASH — REGULATORY / FINANCIAL | OBBA Medicaid Restructuring — Multiple 2026 Provisions Now Effective

The One Big Beautiful Bill Act (H.R. 1, signed 4 Jul 2025) is now in active implementation. Key 2026 provisions: (1) Enhanced FMAP 90% match for Medicaid expansion sunsets 1 Jan 2026 — states absorbing higher costs now. (2) Oct 1, 2026: Medicaid eligibility narrowed for certain non-citizens including refugees and asylees. (3) Dec 31, 2026: Semi-annual eligibility redeterminations required; Medicaid expansion retroactive eligibility cut from 90 to 30 days. Work requirements begin Jan 2027 but state systems must be built now. CBO: 11.8M projected to lose Medicaid coverage by 2034; KFF: ~\$500B in Medicare PAYGO sequestration cuts triggered 2026-2034 including 4% hospital payment reduction unless Congress acts. Medicaid accounts for a median 15% of nonprofit hospital gross revenue — and 54% for children's hospitals. CFOs must model 2027-2028 revenue scenarios NOW.

⚡ FLASH — REGULATORY | HIPAA Security Rule Final Rule Expected May 2026 — Biggest Cybersecurity Mandate in Healthcare History

The HHS OCR HIPAA Security Rule NPRM (issued 27 Dec 2024, first major update since 2013) is on track for final rule publication in May 2026. Coalition of 100+ hospital systems and provider associations called for withdrawal, citing crushing compliance burden. Outcome uncertain under Trump administration's deregulatory posture — but OCR has not withdrawn the rule. If finalized as proposed: ALL implementation specifications become mandatory (no more 'addressable' flexibility). Required within 180 days of publication: MFA for all ePHI access, encryption at rest and in transit, vulnerability scans every 6 months, annual penetration testing, 72-hour system recovery capability, annual business associate verification. Healthcare data breaches average \$10.93M — the highest of any industry. Start gap analysis now regardless of final rule outcome.

LEGISLATIVE & REGULATORY TRACKER — 4-LANE ANALYSIS — 31 MARCH 2026

Tracking active items across four regulatory lanes: Federal Legislative, Federal Regulatory (CMS/HHS/OCR), Accreditation & Standards, and State Regulatory. Current as of 31 March 2026.

LANE 1: FEDERAL LEGISLATIVE

Item	Lane	Status	Action Required	Key Date
OBBBA — Enhanced FMAP Sunset (Medicaid expansion 90% match ends)	Fed Leg	EFFECTIVE	Model revenue impact of higher state share on expansion populations	1 Jan 2026 (LIVE)
OBBBA — Non-citizen Medicaid/CHIP eligibility narrowed (refugees, asylees, etc.)	Fed Leg	EFFECTIVE DEC 2026	Identify affected patient populations; model uncompensated care increase	1 Oct 2026
OBBBA — Semi-annual redeterminations + retroactive eligibility cut (90 to 30 days)	Fed Leg	EFFECTIVE DEC 2026	Prepare for increased uninsured volume; update charity care and collections policies	31 Dec 2026
OBBBA — Work requirements for Medicaid expansion adults (80 hrs/month)	Fed Leg	HHS interim final rule due Jun 2026; requirements begin Jan 2027	Build state systems now; plan for disenrollment cascade and uncompensated care surge	1 Jan 2027
OBBBA — DSH payment reduction delay (to 2029)	Fed Leg	ENACTED — favorable	No immediate action; note that delay expires 2029 — begin 3-yr financial planning	Expires 2029
OBBBA — Medicare PAYGO sequestration (~\$500B; 4% provider cuts)	Fed Leg	Triggered — Congress must act to avoid	Engage advocacy organizations; monitor appropriations process closely	2026-2034
Medicare Advantage 2026 Rate Notice — finalized	Fed Leg	EFFECTIVE	Model MA enrollment shifts affecting hospital mix and revenue	Effective now
Housing for the 21st Century Act — FHA access expansion	Fed Leg	Passed House 390-9; Senate cmt	Monitor for community health housing nexus; SDOH strategy impact	Senate TBD

LANE 2: FEDERAL REGULATORY (CMS / HHS / OCR / FDA)

Item	Agency	Status	Action Required	Key Date
HIPAA Security Rule NPRM — Final Rule Expected	HHS OCR	Final rule expected May 2026; 180-day compliance window	Begin gap analysis NOW: MFA, encryption at rest/transit, vuln scans, pen testing, 72-hr recovery	~Nov 2026 enforce

HIPAA Privacy Rule Update — Tribal consultation Feb 2026	HHS OCR	Active — final rule timing uncertain under Trump admin	Monitor; reproductive health privacy and patient data access changes pending	TBD 2026
CIRCA — Mandatory Cyber Incident Reporting (72 hrs to CISA)	CISA / DHS	Final rules due May 2026	Healthcare is covered critical infrastructure — 72-hr breach reporting and 24-hr ransomware payment reporting	May 2026 final
340B Rebate Model RFI — HRSA seeking stakeholder input	HRSA	RFI open — comment deadline extended to 20 Apr 2026	Submit comments; model revenue impact of rebate model vs. upfront discount	20 Apr 2026
340B Child Site Advance Registration — Court vacated HRSA requirement	HRSA / Federal Court	Vacated 3 Mar 2026; federal govt has 60 days to appeal	Restore previously de-registered child sites; monitor appeal deadline	~2 May 2026
OPPS Drug Acquisition Cost Survey (CMS)	CMS	Survey closes 31 Mar 2026 (TODAY)	Respond strategically — non-response may result in CMS imputing minimum acquisition costs	TODAY 31 Mar
CY 2026 OPPS Final Rule — 2.6% net update; site-neutral drug admin	CMS	EFFECTIVE 1 Jan 2026	Assess site-neutral drug administration payment impact on off-campus PBDs	Effective now
OPPS -0.5% non-drug offset (340B remedy recoupment)	CMS	EFFECTIVE; accelerates to ~2% in 2027 OPPS	Model 2027 impact; begin cost reduction planning for affected hospital outpatient segments	2027 OPPS rule
AI/ML Medical Device — FDA guidance evolving	FDA	Multiple guidances active; no single final framework	Governance review for any AI diagnostic or decision-support tools deployed; FDA submissions review	Ongoing
CMS Innovation Center — GLOBE Model (proposed)	CMS CMMI	Proposed — comment period	Assess applicability for primary care value-based arrangements	TBD

LANE 3: ACCREDITATION & STANDARDS (JOINT COMMISSION / DNV / CMS CoPs)

Item	Body	Status	Action Required	Key Date
Joint Commission — Cybersecurity Standards (EC.02.04.03)	TJC	Active — aligned with NIST CSF	Map current cybersecurity program to TJC standards; survey prep should include cyber resilience documentation	Ongoing

Joint Commission — AI in Clinical Care Standards development	TJC	In development — not yet finalized	Monitor; governance framework for AI tools should be established now ahead of standards	TBD 2026-27
CMS Conditions of Participation — Emergency Preparedness	CMS CoPs	Active — annually tested	Ensure annual EP exercise completed; include cyber disruption scenario as required active threat vector	Annual
CMS Conditions of Participation — Infection Control (post-COVID update)	CMS CoPs	Active	Verify current CoP compliance; post-PHE regulatory posture has shifted back toward enforcement	Ongoing
DNV / NIAHO — Cybersecurity and EHR resilience	DNV	Active in accreditation surveys	For DNV-accredited facilities: cyber resilience documentation is an active survey element	Ongoing

LANE 4: STATE REGULATORY (SELECT HIGH-IMPACT ITEMS)

Item	State(s)	Status	Action Required	Key Date
Medicaid work requirement implementation — state system build	All expansion states	HHS interim final rule due Jun 2026; states must build systems	State Medicaid agency outreach; understand local implementation timeline and disenrollment projection	Jun 2026 rule
State AG consumer protection enforcement (CFPB void)	NY, CA, MA, MI	Active — Capital One \$425M NY AG settlement as model	Audit patient billing, collections, financial assistance policies for state UDAAP exposure	Ongoing
340B contract pharmacy state laws (MN, HI, LA upheld in courts)	Multiple	State laws upheld in multiple circuit courts	Verify compliance with applicable state 340B contract pharmacy laws	Ongoing
Safe staffing / nurse-to-patient ratio legislation	CA active; NY, IL pending	CA mandatory; other states advancing	Multi-state systems: track ratio requirements by state; model labor cost impact	State-specific
Scope of practice expansion (NP/PA independence)	26+ states	Many enacted; federal legislation not advancing	Update credentialing, supervision, and care delivery model for applicable states	State-specific
Certificate of Need (CON) reform	Multiple states	Active legislative changes in several states	Monitor for CON law changes in operating states — affects	State-specific

			capital expansion planning	
--	--	--	----------------------------	--

SECTOR: CYBER THREAT — HEALTHCARE SECTOR SPECIFIC

The healthcare sector has moved from being a high-value ransomware target to being a confirmed geopolitical military objective. The distinction matters operationally: financially-motivated ransomware actors negotiate. Iran-linked actors in the current conflict environment are deploying wiper malware with no ransom demand — the objective is destruction and operational disruption, not extortion. The Stryker attack is the proof of concept. A second healthcare provider has already been hit. Hospitals should expect this pattern to intensify.

The Stryker Attack — Operational Lessons for Hospital Systems

Element	Detail / Lesson
Attack vector	Compromised Microsoft Intune administrator account — legitimate cloud device management platform weaponized. No custom malware initially required.
Impact	200,000+ devices factory reset across 79 countries simultaneously. Ordering, manufacturing, shipping disrupted. Maryland paramedics lost ECG transmission to hospitals.
Attribution	DOJ formal attribution to Iran MOIS (Handala Hack persona) — 21 Mar 2026. FBI seized four domains; Handala launched replacement infrastructure within hours.
Patient safety	Paramedic ECG transmission disruption is a life-safety event, not an IT event. Supply chain disruption has caused surgical delays and procedure cancellations.
Key lesson	Admin credential compromise of a cloud management platform is sufficient to cause enterprise-wide destruction. MFA on ALL admin accounts is non-negotiable.
Pattern signal	Second unnamed US healthcare company hit with Iranian-linked destructive ransomware (no ransom demanded). Halcyon: deliberate focus on the medical sector.

Priority Cyber Control Actions — Healthcare

Control Action	Priority
Audit ALL cloud device management admin accounts (Intune, Jamf, SCCM, etc.) — enforce MFA	IMMEDIATE — Stryker attack vector; this is the specific lesson from the confirmed incident
Verify Stryker equipment network connectivity — assess disconnect/reconnect protocol	IMMEDIATE — Hospitals were left uncertain about whether to disconnect Stryker equipment from networks
Review vendor/third-party connections to clinical networks	IMMEDIATE — AHA: adversaries have 'mapped the sector' and identified mission-critical third-party providers

Validate offline backups for EHR, PACS, pharmacy, and clinical systems	HIGH — Wiper malware confirmed active; offline/immutable backups are the only viable recovery path
Activate H-ISAC threat intelligence membership and verify feed currency	HIGH — H-ISAC is coordinating sector-specific IOC distribution; CISA at 38% staffing makes this essential
Begin HIPAA Security Rule gap analysis against proposed mandatory controls	HIGH — Final rule expected May 2026; 180-day compliance window means ~Nov 2026 enforcement
Conduct tabletop exercise with wiper/destructive attack scenario (not just ransomware)	MODERATE — Most hospital incident response plans model ransomware negotiation; wiper scenario is fundamentally different
Review CIRCIA reporting obligations — 72-hr to CISA, 24-hr for ransomware payments	MODERATE — Final mandatory reporting rules due May 2026; begin internal reporting workflow now

PATIENT SAFETY VECTOR: Cyber disruption affecting connected medical devices, EMS communication platforms, and pharmacy systems is a patient safety event — not just an IT event. Incident command activation protocols should include cyber disruption as a trigger condition.

SECTOR: FINANCIAL PRESSURE — REIMBURSEMENT & REVENUE ENVIRONMENT

Hospital financial conditions in 2026 are being squeezed from multiple directions simultaneously. The OBBBA Medicaid restructuring is not a future risk — it is an active reimbursement event with provisions effective now and accelerating through the end of 2026 and into 2027. The 340B program is under simultaneous attack from HRSA, CMS, and pharmaceutical manufacturers. The OPDS drug acquisition cost survey closed today and will likely inform future payment reductions. Institutions that model their 2027-2028 revenue on 2025 reimbursement assumptions are building plans on a crumbling foundation.

OBBBA Medicaid Financial Impact — Hospital Exposure Assessment

Hospital Type	Financial Exposure
Children's hospitals	HIGHEST — Medicaid = 54% of median gross revenue. Work requirements and eligibility restrictions disproportionately affect pediatric Medicaid population.
Safety-net / DSH hospitals	CRITICAL — Largest uncompensated care burden increase. \$50B rural hospital fund provides partial cushion but urban safety-net hospitals excluded.
Rural hospitals	HIGH — \$50B Rural Hospital Transformation Fund (\$10B/yr 2026 on) provides some offset. Distribution methodology still being developed.
Urban safety-net / city-county hospitals	CRITICAL — DSH payment protections delayed to 2029 but base Medicaid volume at risk. Provider tax restrictions compound financial pressure.
Nonprofit systems w/ high commercial mix	MODERATE — Direct Medicaid exposure lower; however uncompensated care cost-shifting and workforce impacts are secondary risks.
Academic medical centers	MODERATE-HIGH — GME funding unaffected but Medicaid patient volume decline affects clinical training capacity and research cross-subsidies.

340B Program — Active Threat Summary

- OPSS Drug Acquisition Cost Survey closes TODAY (31 March 2026). Non-response risks CMS imputing minimum acquisition costs — which will be used to set 2027 reimbursement rates. Consult advisors immediately if not yet responded.
- 340B Rebate Model RFI comment deadline: 20 April 2026. HRSA is actively exploring a shift from upfront discounts to a back-end rebate model — which would require covered entities to 'float' drug costs to manufacturers, creating cash flow disruption. AHA is mobilizing opposition. Submit institutional comments.
- Child site court ruling (3 March 2026) vacated HRSA's advance registration requirement — favorable for covered entities. Federal government has until ~2 May 2026 to appeal. Restore previously de-registered child sites now while ruling is in effect.
- Manufacturer contract pharmacy restrictions continue to escalate. Novo Nordisk, Eli Lilly, and others are implementing new claims-data submission policies on 340B hospitals. AHA filed opposition (3 March 2026). Track applicable manufacturer policies for your formulary.
- CMS drug acquisition cost survey data (due today) will inform 2027 OPSS payment rates for Part B drugs. 340B covered entities with lower acquisition costs face higher risk of rate reduction. The 0.5% non-drug OPSS offset is expected to accelerate to ~2% in the 2027 OPSS rule.

SECTOR: WORKFORCE & LABOR CONTINUITY

Healthcare workforce stability is under simultaneous pressure from three converging forces: a structural pre-existing shortage in nursing and physician supply, active immigration enforcement operations creating fear and departure among foreign-born clinical staff, and the military reserve activation associated with Operation Epic Fury drawing skilled healthcare workers (combat medics, nurses, corpsmen) from civilian hospital systems.

Immigration Enforcement Impact on Healthcare Workforce

Workforce Segment	Exposure Level	Operational Impact
Foreign-born physicians (26% of US physician workforce)	HIGH — visa uncertainty, deportation fear, international recruitment disrupted	Rural hospitals already reporting physician departures to Canada and other countries; West Virginia: near 1-in-5 nursing vacancies
Foreign-born registered nurses (16% of RN workforce)	HIGH — Philippines, India, African countries primary pipeline	International nurse recruitment programs disrupted; visa processing delays causing last-minute job offer rescissions
Undocumented healthcare workers (~366,000)	CRITICAL for home health/nursing homes — 40% of home health aides are foreign-born	Rural and long-term care facilities face most acute exposure; home health referral-to-admission rate already 55%
H-1B visa holders (physicians in GME)	ELEVATED — fee increases, stricter eligibility	Teaching hospitals: GME pipeline affected; J-1 waiver program delays compounding
US military reserve / National Guard activations	MODERATE — Epic Fury mobilization ongoing	Combat medics, nurses, and corpsmen being activated; most acute in National Guard-heavy regions

Workforce Operational Recommendations

- Conduct immediate headcount audit of visa-status clinical staff. Identify roles where departure would create patient safety gaps and activate contingency staffing plans.
- Accelerate H-1B and immigrant visa processing for pending international recruits — delays are creating last-minute rescissions. Budget for premium processing fees.
- For rural hospitals: engage state Medicaid agency now regarding 340B rural provisions and state flex programs — these are the financial cushion that determines survival under OBBBA.
- Model overtime and agency/travel nurse cost exposure for 2026-2027 under worst-case workforce departure scenario. Travel nurse rates remain elevated relative to pre-COVID levels.
- Review military leave policies and coverage plans for reserve/Guard-activated clinical staff; activation periods under Epic Fury are expected to span months.

SECTOR: SUPPLY CHAIN & MEDICAL DEVICE AVAILABILITY

The healthcare supply chain faces dual disruption in Q2 2026: geopolitical cyber targeting of medical device manufacturers (Stryker confirmed; second company confirmed by Halcyon) and the Strait of Hormuz closure creating pharmaceutical input cost pressure and logistics delays for imported medical supplies and devices. The Stryker attack demonstrated that cyber disruption of a device manufacturer directly translates to surgical delays and patient care deferrals at hospital level.

Current Supply Chain Risk Assessment

Supply Category	Risk Level	Current Assessment
Stryker medical devices / surgical equipment	CRITICAL	Ordering and shipping systems disrupted since 11 Mar; surgical delays confirmed. Verify alternative vendor relationships for critical surgical components now.
Second unnamed medical device vendor	HIGH	Halcyon confirmed second US healthcare company hit with Iran-linked ransomware. Identity not public. Audit critical vendor cyber posture immediately.
Pharmaceutical inputs via Hormuz corridor	ELEVATED	LNG disruption affects energy-intensive pharmaceutical manufacturing. Monitor API (active pharmaceutical ingredient) supply for Hormuz-dependent synthetics.
Medical device components (semiconductors, industrial gases)	ELEVATED	Helium (Qatar Ras Laffan) at 90-day depletion window. Semiconductor supply risk. Monitor FDA medical device shortage tracking weekly.
EMS / emergency communications equipment	ELEVATED	Stryker Lifenet (ECG transmission) disruption confirmed. Evaluate backup ECG transmission protocols with EMS partners.
Blood / biologics	MODERATE	ARC blood logistics not currently disrupted. Monitor HHS emPOWER and ARC supply bulletins weekly during active conflict period.
PPE / consumables supply chain	NOMINAL	Post-COVID domestic stockpile programs operational. No current significant disruption. Maintain standard 30-day buffer inventory.

Supply Chain Control Actions

- Stryker equipment: Establish direct communication with your Stryker rep for real-time system recovery status. Identify alternative vendors for critical surgical implants and equipment that may be on backorder.
- Conduct vendor cyber resilience review for all medical device manufacturers with network-connected products in your facilities. Ask specifically: do they use cloud-based device management (Intune, Jamf)? What is their MFA posture for admin accounts?
- Activate FDA MedWatch device shortage monitoring for any implant categories dependent on Stryker supply chain. Cross-reference with elective surgery scheduling.
- For devices with direct patient connectivity (infusion pumps, ventilators, monitors): verify network segmentation is current and isolate any devices from internet-facing network segments pending vendor security confirmation.

72-HOUR OPERATIONAL OUTLOOK (31 Mar – 03 Apr 2026)

Horizon	Assessment
0–24 Hours	OPPS drug acquisition cost survey CLOSES TODAY. Submit if not yet done. H-ISAC threat feed. Monitor Stryker supply chain update. Watch for additional Iranian cyber activity against healthcare targets.
24–48 Hours	340B RFI comment period approaches (20 Apr deadline). Watch for HHS announcements on HIPAA Security Rule timeline. Monitor for third confirmed Iranian cyber event against healthcare sector.
48–72 Hours	Monitor: Pakistan diplomatic channel for ceasefire signals — would reduce cyber threat posture but supply chain disruption lag remains weeks. CIRCIA final rule expected May; watch for pre-publication announcements. AHA advocacy response to OBBBA work requirements interim final rule (due Jun 2026).

Escalation Threshold: A third confirmed Iranian cyber event against a US hospital or health system (vs. device manufacturer) would represent direct patient safety infrastructure targeting and should trigger immediate activation of incident command and board notification protocols.

WATCH LIST — INDICATORS TO MONITOR NEXT 7–14 DAYS

- Confirmed cyberattack against a US hospital's EHR or clinical information system (vs. device manufacturer) — represents direct patient safety event threshold.
- Identity of second Halcyon-confirmed healthcare company victim becomes public — signals acceleration of disclosure norm and potential class-action exposure.
- HIPAA Security Rule final rule publication in Federal Register — starts 60-day effective date clock and 180-day compliance window.
- CIRCIA final rules published (expected May) — review 72-hour reporting obligations for healthcare critical infrastructure.
- HHS interim final rule on Medicaid work requirements (due Jun 2026) — states must begin building systems immediately upon publication.
- 340B rebate model RFI comment period closes 20 April — monitor AHA and industry coalition response for strategic signal on HRSA direction.
- Stryker supply restoration timeline update — any announcement of extended disruption triggers surgical scheduling review and alternative vendor activation.

- State Medicaid work requirement implementation announcement — any state announcing early system build or waivers affects patient population projections.

COLLECTION INTELLIGENCE LOG — 31 MARCH 2026

Sources consulted in preparation of this edition. Tier designations per Fortune Favors the Prepared Source Registry v1.5.

Source	Tier	Coverage / Key Data
State of Surveillance / DOJ / HIPAA Journal — Stryker attack	T1	200k devices wiped; DOJ attribution 21 Mar; Maryland paramedic impact
Halcyon / Cybersecurity Dive / Healthcare Brew	T1	Second US healthcare company hit; deliberate medical sector targeting pattern
CNN / Chief Healthcare Executive / Washington Times	T1	Stryker impact on hospital decisions; Iranian cyber pattern; AHA commentary
Foley & Lardner / Unit 42 / SISA — cyber legal/intelligence	T1	CIRCA obligations; healthcare sector threat landscape; control actions
AMA / KFF / Commonwealth Fund — OBBBA analysis	T1	Medicaid cut projections; hospital financial exposure; 11.8M uninsured estimate
HFMA / Fierce Healthcare / Healthcare Finance News	T1	Hospital financial impact modeling; safety-net exposure; DSH analysis
HRSA.gov — 340B program updates (Feb-Mar 2026)	T1	RFI; child site ruling; rebate model court decision (10 Feb 2026)
CMS / America's Essential Hospitals — OPSS 2026 final rule	T1	340B survey; site-neutral payments; 2.6% update; drug admin cuts
Forvis Mazars / Chartis / K&L Gates — 340B analysis	T1	Current 340B program state; covered entity strategic implications
HIPAA Journal / MedicalITG — HIPAA Security Rule	T1	NPRM status; May 2026 final rule timeline; mandatory controls summary
HHS OCR Federal Register — HIPAA Security Rule NPRM (6 Jan 2025)	T1	Primary regulatory source for security rule requirements
NPR / Niskanen / Akin Gump / NPZ Law — workforce / immigration	T1	1.1M noncitizen healthcare workers; physician departure pattern; H-1B impact
Davis Vanguard / VisaMadeEZ — rural workforce impact	T2	West Virginia case study; international nurse recruitment disruption
H-ISAC / AHA — cybersecurity advisories	T1	Sector-specific threat coordination; Stryker response guidance

— END OF REPORT —

SUBSCRIBE TO THE DTR BUSINESS EDITION

*Operational intelligence built for healthcare executives — CFOs, COOs, CISOs, and risk officers
who need to act, not just monitor.*

Enterprise licensing | System-specific briefings | 4-lane legislative tracker |
fortunefavorstheprepared.com

fortunefavorstheprepared.com

Semper Paratus. Semper Gumby.