perplexity

Cyber-Insurance Readiness Checklist for Hospital CIO/CISO Teams

This checklist distills the controls U.S. cyber-insurance underwriters most frequently flag in 2025 healthcare submissions. For each control you'll find:

- Required documentary evidence to satisfy underwriting questionnaires or follow-up audits
- A recommended internal review cadence that aligns with broker expectations and regulatory guidance

> Tip: Maintain a single "underwriting evidence binder" (digital or GRC platform folder) and update it on the cadences below; doing so accelerates renewals and reduces claim-denial risk.

1. Identity & Access Management

Control	Evidence to Supply Underwriter	Review Cadence
Multi-Factor Authentication (MFA) for all privileged, remote and email access	- MFA architecture diagram - Screen captures of enforcement settings (Azure AD / Okta policies) - Sample authentication logs showing successful MFA challenges in last 30 days	Monthly log spot-check; full configuration attestation quarterly [1] [2]
Privileged Access Management (PAM) / Least Privilege	- Inventory of privileged accounts with role descriptions - PAM tool report showing password rotation & session recording enabled - Last quarterly audit of admin rights on endpoints	Quarterly audit; real-time alerts for new privileged accounts [3] [4]
Zero-Trust Segmentation / Network Micro-segmentation	- Network map highlighting patient-care VLANs, IoT/medical-device zones, and admin networks - Policy set from NAC/ZTNA platform showing default-deny rules - Last penetration-test summary validating lateral-movement prevention	Semi-annual rule review; annual third-party pen test [5] [6]

2. Endpoint & Network Security

Control	Evidence to Supply Underwriter	Review Cadence
Endpoint Detection & Response (EDR/XDR) across servers, clinician workstations, medical devices (where feasible)	- Vendor coverage report (% of endpoints protected) - 24×7 SOC alert sample & runbook - Last EDR containment test results	Monthly coverage gap scan; bi-annual containment drill [7] [8]
Vulnerability & Patch Management (critical CVEs ≤30–90 days per device class)	- Automated scan reports showing age of open critical/high CVEs - Change-control records for OS & device firmware patches - Risk-based exception list (e.g., FDA-restricted devices)	Monthly scans; board metrics quarterly [9] [10] [11] [12]
Unsupported / End-of-Life System Mitigation	- Asset list of EOL systems with compensating controls (isolation, ACLs) - Vendor statements of extended support contracts - Migration roadmap with milestones	Semi-annual review; update insurer if inventory changes >10% [13]

3. Data Resilience & Recovery

Control	Evidence to Supply Underwriter	Review Cadence
Immutable, Air-Gapped or Isolated Backups (“3-2-1” with immutability)	- Backup architecture diagram showing off-network or object-lock targets - Immutable-switch configuration screenshots - Last successful restore test report (RTO/RPO achieved)	Quarterly restore tests; monthly backup integrity check [14] [15] [16]
Backup MFA & Credential Segregation	- Proof that backup admin accounts use MFA and differ from domain creds - Privileged credential vault logs for backup systems	Quarterly access audit [15]
CBI (Contingent Business Interruption) Exposure Mapping	- Dependency map of top 10 external SaaS/cloud/EHR vendors - Contact list & BAA copies for each critical provider	Annual map update; after onboarding new Tier-1 vendor [17]

4. Incident Response & Tabletop Exercises

Control	Evidence to Supply Underwriter	Review Cadence
Written Incident Response (IR) Plan aligned to HHS Cybersecurity Performance Goals (CPGs)	- Signed IR plan with RACI matrix - List of pre-approved breach counsel, forensics, PR vendors	Annual formal update; ad-hoc after major changes [18] [19]

Control	Evidence to Supply Underwriter	Review Cadence
Tabletop Exercises covering ransomware, third-party outage, data-exfiltration	- Agenda, scenario scripts, attendee list (incl. executives), and after-action report - Tracker of remediation items with status	At least annually; every 6 months for large IDNs or after material incidents [20] [21] [22] [23]
48-Hour / SEC 4-Day Disclosure Playbook	- Workflow diagram aligning IR steps with parallel legal/SEC notice duties - Template Form 8-K / state breach letters	Review after each major regulation change; drill in tabletop [24] [25]

5. Security Awareness & Human Layer Controls

Control	Evidence to Supply Underwriter	Review Cadence
Workforce Security Awareness & Phishing Simulation	- LMS completion reports (≥90% staff within last 4 months) - Phish-test metrics (click rates, repeat offenders coaching)	Quarterly mini-modules; phishing tests at least monthly [26] [27] [28]
Social-Engineering / Funds-Transfer Fraud Procedures	- Dual-control treasury SOPs - Call-back verification logs for wire requests over threshold	Annual policy review; monthly QA sampling [29] [30]

6. Third-Party & Medical Device Security

Control	Evidence to Supply Underwriter	Review Cadence
Vendor / Third-Party Risk Assessment Program	- Risk-tiering methodology and inventory - Completed security questionnaires & SOC 2/HITRUST reports for Tier 1 vendors - Tracking dashboard of remediation status	Initial onboarding plus annual reassessment of Tier 1; continuous external-attack-surface monitoring [31] [32]
FDA 524B Cyber Device Plan & SBOM Tracking	- Cyber-device inventory with patch constraints - Manufacturer security documentation & SBOMs - Compensating controls register	Semi-annual review; update upon new device procurement [33] [34]
Medical IoT Network Segmentation & Passive Monitoring	- Tool reports showing device discovery and abnormal traffic alerts - Policy mapping medical VLANs to firewall rules	Quarterly device discovery scan; annual rule recertification [35]

7. Governance, Audit & Continuous Compliance

Control	Evidence to Supply Underwriter	Review Cadence
Enterprise Risk Analysis (HIPAA / NIST CSF)	- Signed risk analysis with risk-rating heatmap - Board minutes acknowledging review	Annually; major refresh after mergers or EHR overhaul [36] [37]
Continuous Compliance Monitoring & Metrics	- Dashboard screenshots (MFA coverage, patch SLAs, training completion) exported within last 30 days - Ticketing evidence of remediation follow-ups	Monthly dashboard submission to CISO; quarterly report to board and broker [38] [39] [40]
Policy Exception & Misrepresentation Controls	- Formal process for documenting security control exceptions - Attestation form signed by CISO & CFO for insurance application accuracy	Exception log review quarterly; attestations at renewal and mid-term changes [41] [42]

Putting It Into Practice

1. **Assign owners now.** Each checklist line must have a named control owner; underwriters may ask for that org chart.
2. **Digitize evidence.** Scan or export every artifact in PDF; keep version history. GRC or secure SharePoint with broker access is ideal.
3. **Link cadence to calendar.** Automate reminders 30 days before each review cycle and tie to incident-response runbook.
4. **Update mid-term.** If a control materially degrades (e.g., new EOL system added, tabletop delayed), notify your broker promptly—non-disclosure is a top claim-denial cause [30] [41].

Following this structured cadence and evidence model positions hospitals to:

- Qualify for broader limits at lower retentions
- Avoid restrictive exclusions tied to unsupported systems or failed controls
- Defend claims with clear proof of ongoing due diligence

Keep the binder current, and renewal season becomes a data export—not a scramble.

⁂

1. https://www.garrishorn.com/blog/xfmo575g0whus4xir8kryjwnsa3dq8
2. https://blog.gomainspring.com/it-security/your-cyber-insurance-and-mfa-requirements
3. https://www.ssh.com/blog/how-to-do-privileged-access-management-audit
4. https://www.ignition-technology.com/wp-content/uploads/2024/02/BT_WhitePaper_PAM-Buyers-Guide-2023.pdf
5. https://www.stocktitan.net/news/ZS/zero-trust-security-reduces-cyber-insurance-claims-preventing-up-to-f0fgjnznbhlj.html
6. https://ipservices.com/2025/03/20/cyber-insurance-wont-save-you-but-zero-trust-can/
7. https://sentinelra.com/blog/employing-mfa-and-edr-to-strengthen-cybersecurity-and-minimize-risk

8. https://www.exabeam.com/blog/siem-trends/how-siem-helps-with-cyber-insurance/
9. https://www.greatamericaninsurancegroup.com/content-hub/loss-control/details/securing-your-systems--the-role-of-patching-cadence-in-cybersecurity
10. https://securityscorecard.com/blog/patch-cadence-and-management-best-practices/
11. https://www.defendify.com/blog/whats-your-testing-frequency/
12. https://www.indusface.com/blog/how-often-to-run-vulnerability-scans/
13. https://stonefly.com/blog/get-cyber-insurance-with-immutable-backups/
14. https://www.alvaka.net/automated-backup-solutions-for-ransomware-a-shield-against-cyber-threats/
15. https://www.cyberinsuranceacademy.com/blog/guides/boosting-your-insureds-cyber-resilience-with-data-backups/
16. https://woodruffsawyer.com/insights/cyber-insurance-requirements-next-frontier
17. https://www.bbrown.com/us/insight/cyber-coverage-handbook-medical-devices-risks/
18. https://www.mintz.com/insights-center/viewpoints/52541/2024-04-04-hhs-health-care-cybersecurity-performance-goals
19. https://www.hipaajournal.com/hph-cybersecurity-performance-goals/
20. https://woodruffsawyer.com/insights/cyber-101-tabletop-webinar
21. https://docket.acc.com/node/4228
22. https://www.alertmedia.com/blog/tabletop-test/
23. https://www.epiqglobal.com/en-us/resource-center/articles/healthcare-organizations-can-meet-new-hhs-cybersecurity-goals-with-the-help-of-tabletop-exercises
24. https://www.healthlawadvisor.com/recent-developments-in-health-care-cybersecurity-and-oversight-2024-wrap-up-and-2025-outlook
25. https://www.linkedin.com/pulse/roping-risk-what-your-cyber-planning-cadence-chris-cpat-patteson--0vehe
26. https://blog.usecure.io/how-often-should-employees-really-receive-security-awareness-training
27. https://www.terranovasecurity.com/blog/security-awareness-training-frequency
28. https://isgovern.com/blog/how-often-do-you-need-to-train-employees-on-cybersecurity-awareness/
29. https://www.ajg.com/news-and-insights/2022/jan/top-9-areas-of-focus-for-cyber-insurance-underwriters/
30. https://alliant.com/news-resources/article-navigating-the-cyber-insurance-claims-process/
31. https://www.upguard.com/blog/vendor-risk-assessment
32. https://www.upguard.com/blog/how-to-perform-a-third-party-risk-assessment
33. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs
34. https://www.greenlight.guru/blog/cybersecurity-medical-device
35. https://www.cm-alliance.com/cybersecurity-blog/bolstering-cybersecurity-in-healthcare-with-cyber-tabletop-exercises
36. https://www.techtarget.com/healthtechsecurity/feature/How-healthcare-CISO-responsibilities-are-evolving
37. https://www.upguard.com/blog/preparing-for-cybersecurity-audits
38. https://www.upguard.com/blog/compliance-monitoring

39. https://thehackernews.com/2025/03/why-continuous-compliance-monitoring-is.html
40. https://www.infrascale.com/cyber-insurance-statistics-usa/
41. https://www.holmesmurphy.com/blog/the-impact-of-multi-factor-authentication-on-cyber-insurance/
42. https://www.crawco.com/blog/bridging-the-mfa-gap-in-cyber-insurance