RISK INSIGHTS

HEALTH CARE INDUSTRY TRENDS TO WATCH IN 2026

Health care organizations enter 2026 facing numerous operational, financial and liability pressures, including labor shortages, inflation, supply chain volatility and the impact of U.S. tariffs on pharmaceutical imports. Although the commercial insurance market has generally softened, several segments remain affected by persistent loss severity and loss control challenges. In particular, social inflation and large liability awards continue to pressure the medical professional liability (MPL) space, while rising ransomware activity and escalating third-party cyber incidents may affect cyber coverage. As such, health care providers with high-risk exposures or less mature risk management controls may encounter tighter underwriting, higher deductibles or reduced capacity.

To secure the best insurance terms, organizations should stay abreast of market developments and strengthen their loss-control measures. This article highlights the top trends shaping health care risk in 2026, examines their impact on insurance, and offers risk management and coverage strategies.

CYBER RISK EVOLVES INTO A BUSINESS INTERRUPTION AND VENDOR DEPENDENCY

Cybersecurity remains a critical concern as health care data breaches continue to escalate. According to Fortified Health Security's 2026 Horizon Report, the sector experienced more than twice as many breaches in 2025 as it did in 2024. Ransomware groups increasingly target clinical workflows, recognizing that disruptions to patient care may pressure affected organizations to pay ransoms. Threat actors are also targeting third-party vendors, including clearinghouses, electronic health record platform hosts and managed service providers. A single point of failure anywhere in the supply chain can leave organizations unable to submit health care claims, receive reimbursement or validate insurance coverage, disrupting operations and straining revenue cycles.

Robust cybersecurity measures (e.g., network segmentation, multifactor authentication, access management and endpoint protection) will be essential for patient safety and service continuity in the year ahead and may increasingly be required by underwriters. Organizations should also evaluate the security posture of vendors, establish incident response plans with clear backup and recovery processes, and conduct frequent tabletop exercises to prepare for cyberattacks, including technology provider outages.

Given the continued prevalence of ransomware, organizations should confirm their cyber insurance policies include coverage for extortion and incident response. They should also review cyber business interruption provisions, including dependent business interruption coverage, to confirm whether losses tied to vendor-related incidents are included.

WORKFORCE STRAIN AND WORKPLACE VIOLENCE BECOME ENTERPRISE-LEVEL RISKS

Aging demographics, increased care demands and worker burnout are contributing to workforce strain. An ongoing shortage of health care professionals is placing additional pressure on the sector, with 40% of nurses intending to leave or retire within the next five years, according to the National Council of State Boards of Nursing. Additionally, workplace violence is rising, and health care workers are four to five times more likely to suffer workplace violence injuries than private-sector workers overall, OSHA has found. Collectively, these factors can harm morale, increase staff turnover and disrupt care delivery. Moreover, violent incidents may cause reputational harm and increase organizations' exposure to workers' compensation, general liability and premises liability claims.

Organizations should establish a formal workplace violence prevention program to proactively mitigate and respond to incidents, including clear reporting

RISK INSIGHTS

protocols, patient and visitor code-of-conduct standards, and de-escalation and conflict management training. They should also review their general liability and excess liability policies for assault-and-battery exclusions or other limitations that may restrict coverage for violent altercations.

MPL SEVERITY AND SOCIAL INFLATION PERSIST

Nuclear verdicts exceeding $10 million continue to rise. According to TDC Group, the average of the top 50 medical malpractice verdicts increased from $32 million in 2022 to $48 million in 2023 and $56 million in 2024. Several factors are driving these outsized awards. Attorneys often use aggressive tactics to heighten juror emotion, including reptile-theory strategies, while third-party litigation funding enables plaintiffs to pursue larger, longer and more ambitious cases. In response, insurance carriers may reduce limits, raise attachment points and impose stricter underwriting discipline. Furthermore, health care providers with self-insured retentions may find it difficult to budget for and maintain retained risk layers that reflect today's severity trends.

Organizations should continue to strengthen patient safety and care quality measures to reduce nuclear verdict exposure, with particular emphasis on standardized clinical protocols, reliable communication and handoff practices, and clear care escalation and rapid response procedures. Furthermore, strong governance; early claim reporting; and clear, complete and consistent clinical documentation can proactively improve defensibility. Organizations should also evaluate whether their liability sublimits and excess layers remain adequate in today's severity environment.

AI ADOPTION EXPANDS GOVERNANCE, LIABILITY AND CYBER CONSIDERATIONS

Artificial intelligence (AI)-enabled tools are rapidly expanding, supporting risk prediction, early-deterioration alerts, and imaging analysis, among other applications. Once experimental, many AI pilots are now being integrated into core workflows. In particular, AI is increasingly used for patient communication, clinical documentation and appointment scheduling, easing the administrative demands that contribute to clinician burnout. In fact, 57% of U.S. physicians cite administrative burden as AI's greatest opportunity, according to the American Medical Association.

However, AI may introduce data privacy concerns, cybersecurity exposures and potential diagnostic or workflow errors. As such, organizations should adopt a clear AI strategy that defines desired outcomes and risk tolerances for each use case and is supported by strong governance and human oversight. Vendor scrutiny of third-party AI tools is also essential, with contracts clearly outlining how the tools work and who is accountable when problems arise.

Given AI's risks, organizations should consider how AI-related events might trigger different insurance lines. For instance, cyber policies may address AI-related data breaches, while MPL may address AI-related harm to patients. Reviewing how AI intersects with cyber, MPL, errors and omissions, and directors and officers coverage can help identify potential gaps, exclusions or coverage ambiguity.

CONCLUSION

Several loss-control trends are affecting the health care sector, underscoring the importance of staying informed and adaptive. By tracking these developments and adopting robust risk management practices, health care organizations can increase resilience and maintain operational success.

Contact us today for additional industry-specific risk management guidance.