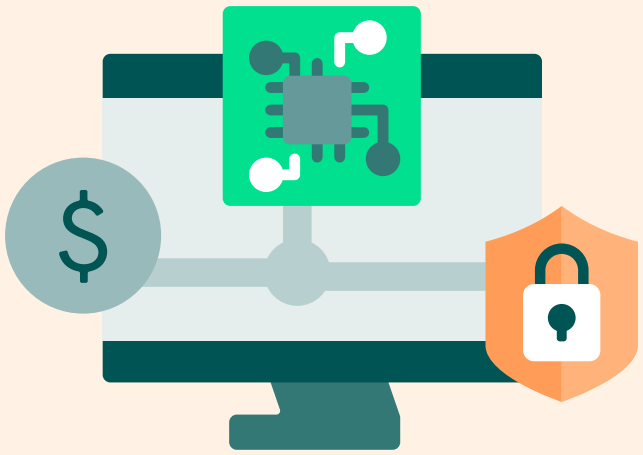
FinThrive™

Checklist for CIOs

Enhancing Revenue Cycle Management with AI and Strengthening Cybersecurity



Healthcare is rapidly transforming, and AI is revolutionizing the industry by delivering enhanced patient experiences, faster processing times and smarter decision-making capabilities.

For hospital and health system CIOs, integrating AI into revenue cycle management (RCM) is no longer optional but essential to ensure financial stability, operational efficiency and long-term resilience.

At the same time, combating cyber threats and managing complex vendor portfolios remain critical challenges.

This checklist offers actionable steps to help CIOs leverage AI-driven automation, strengthen cybersecurity and position their organizations as leaders in healthcare innovation.

Evaluate Vendor Cybersecurity Measures

Why it Matters

Healthcare organizations are prime targets for cyberattacks, with vendor vulnerabilities often serving as entry points for breaches. A comprehensive cybersecurity framework helps safeguard patient data, reduce risk exposure and minimize interruptions.

Action Steps

Conduct thorough security audits of your vendors, focusing on their ability to combat evolving threats

Require evidence of ongoing investments in security measures, such as penetration testing, endpoint protection and employee training programs

Insist on cyber-resilient infrastructures, including secondary environments for rapid recovery, helping to ensure operations can resume within days

Go beyond standard questionnaires by holding face-to-face meetings with vendors to explore their long-term security roadmaps and ransomware prevention plans

Demand security to be an integral part of vendor development, designed right from inception rather than applied after deployment

Consolidate Your Vendor Portfolio for Better Efficiency

Why it Matters

Managing too many vendors increases complexity, security vulnerabilities and inefficiencies. A streamlined vendor portfolio enhances oversight and allows for stronger partnerships that align with organizational goals.

Action Steps

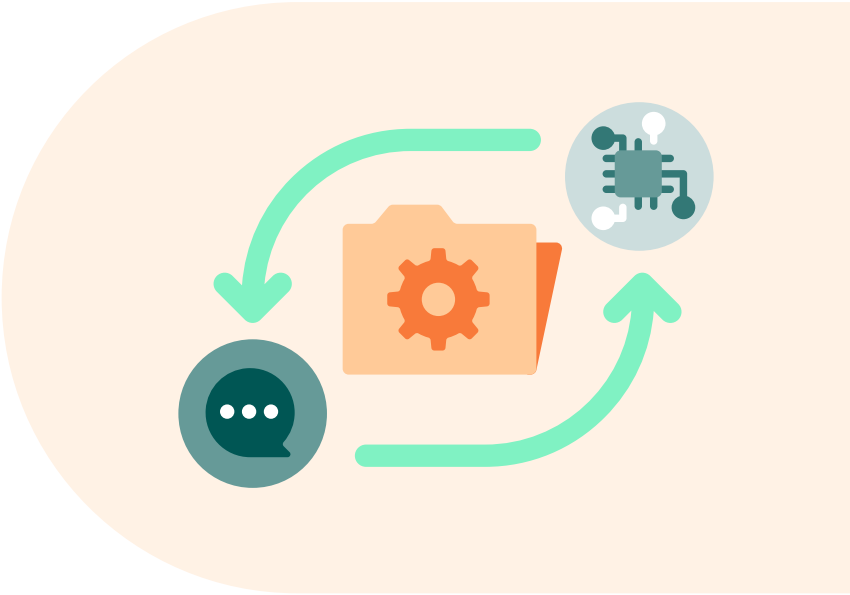
Identify redundancies in your vendor network and prioritize partners who offer robust security and align with your AI-driven strategies

Collaborate with vendors capable of integrating multiple solutions, such as claims processing combined with denial management

Develop a phased multi-year plan to reduce vendor sprawl and shift to a focused group of trusted collaborators — for instance, transition from 100+ vendors to a concentrated portfolio

Stay updated with key vendors on future advancements in AI and cybersecurity through regular strategic reviews

Map Out AI-Driven Automation for RCM Workflows



Why it Matters

Administrative inefficiencies like prior authorization slow patient care and hinder operational efficiency. AI-driven automation eases this burden, results in fewer manual tasks and delivers higher accuracy.

Action Steps

Implement AI tools that dynamically adjust prior authorization rules in response to real-time denial data

Opt for solutions capable of automating repetitive tasks, such as generating appeal letters, to free up your workforce for more strategic roles

Embed AI-driven robotic process automation (RPA) seamlessly into workflows to minimize operational disruptions

Collaborate with vendors experienced in AI for RCM, focusing on areas like denial prediction and claims optimization

Define clear metrics for AI performance monitoring, such as reductions in denial rates, improved authorization turnaround times and clinician satisfaction scores

Test and Refine Cyber-Resilience Plans

Why it Matters

With new cyber threats emerging constantly, cyber resiliency helps ensure your systems can recover quickly from attacks, which is crucial for uninterrupted operations.

Action Steps

- Partner with vendors to build systems that withstand threats like ransomware, incorporating redundancies into your infrastructure
- Regularly simulate breach scenarios to test and refine incident response plans — ensure involvement from IT, clinical and administrative teams
- Assess vendor recovery timelines to ensure they align with operational needs — define clear roles and responsibilities during incidents
- Update response protocols quarterly or bi-annually to reflect new threats and take insights from recent breaches in the industry
- Invest in AI-based monitoring tools that detect anomalies and flag potential threats before they escalate

Next Steps

AI has transitioned from being a promising innovation to a fundamental necessity in healthcare. CIOs must act decisively to integrate AI-driven automation into RCM, improve cybersecurity and modernize vendor management strategies.

Here's how to begin today:

Start small but act now: Identify one immediate area where AI or cybersecurity improvements can make a significant impact

Measure success early by tracking specific metrics, such as denial rates, processing times or resilience test results

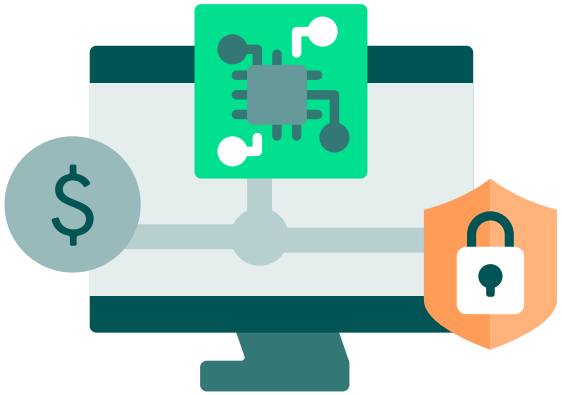
Collaborate with internal teams and trusted vendors to align on implementation priorities

Plan ahead for scalability by building roadmaps that accommodate growth and future advancements in technology

Take the Lead in Innovation

FinThrive is here to partner with you on this transformative journey. With our expertise in AI-driven automation and advanced cybersecurity solutions, we empower providers to streamline operations, mitigate risk and achieve measurable success.

Visit finthrive.com/intelligence and take the first step toward building a smarter, more resilient organization.



FinThrive