




The Promise (and Peril) of AI in Healthcare

5 Best Practices for Managing AI Risks to Safety & Security



Artificial intelligence (AI) has huge potential to transform healthcare for the better, but given AI's unbridled adoption across the industry in just the past year alone, healthcare organizations must begin to actively manage the risks that AI presents to cybersecurity and patient safety. Based on conversations with leading healthcare CIOs, CISOs, and IT/Security teams, here are 5 proven best practices for managing and mitigating the emerging risks of AI across healthcare:

1. Create Centralized, Digital Inventory of AI Vendors

Peter Drucker said "If you can't measure it, you can't improve it", and this readily applies to understanding the full breadth of AI applications already in use (or soon to be in use) across the organization. With thousands of AI products flooding the marketplace, manually managing third-party AI risk with spreadsheets simply isn't feasible – and, in fact, can create significant incremental risk exposure if a critical AI application is missed or remains un-monitored. As such, leading organizations are creating centralized, digital inventories of all AI vendors and products to understand, assess, and manage the full scope of AI risk exposure across the organization.

2. Assess Third – and Fourth – Party AI Risk

With the use of AI already spreading fast across healthcare organizations, understanding the full depth of AI risk exposure begins with asking the right questions. As many AI vendors use *other* AI vendors to train their models and source their data, risk assessments must include both third and fourth party considerations to surface potentially hidden risks.

Key risk assessment questions for AI vendors and products:

- Does the product contain artificial intelligence?
- What are the use cases? How is the AI being deployed?
- Does the product use PHI, PII, PCI for training?
- Is PHI, PII, or PCI sent to a 4th Party AI service? Which?
- Is the data de-identified before sent for training?
- What protections are in place to safeguard the data?
- Upload a Software Bill of Materials (SBOM), if available

3. Leverage Cyber Risk Automation

Leading healthcare organizations leverage automation across the entire assessment workflow process to efficiently and effectively reduce risk. This includes the generation, assignment, and tracking of key risk findings, corrective action plans (CAPs), and targeted remediations for all AI vendors and products. In addition, leading organizations monitor AI risk continuously, including real-time alerts for any material changes in AI vendor security controls as well as breach notifications for any and all AI vendors in their third-party portfolio.

4. Meet the Speed of AI Innovation (and Risk)

While it is imperative to get risk visibility into newly-procured AI applications, many *existing* vendors – already deployed and in use by the business – are rapidly adding AI capabilities. Keeping track of this incremental AI risk can be difficult, time-consuming, and can easily go unnoticed; as such, frequent reassessment of existing vendors and products is critical to monitoring and understanding your organization's ever-expanding AI risk exposure. To ensure the reassessment process keeps pace with AI's evolution, leading organizations automatically schedule and perform reassessments based on assigned risk tiers. For instance, Critical and High-Risk vendors are automatically reassessed every year, at minimum.

5. Educate & Engage the Board on AI

As many Boards find out the hard way, cyber risk is enterprise risk. With AI set to transform almost all aspects of care, CIOs and CISOs have begun educating their Boards on the vast landscape of risks that AI poses to the organization. With most Board members lacking technical expertise, leading CIOs and CISOs have found it useful to communicate cybersecurity in the context of core risk themes that connect back to the business – e.g., Patient Safety, Growth & Strategy, or Financial Health. In addition, many security leaders find it helpful to communicate cyber performance to the Board using peer benchmarking. Demonstrating to the Board how their own organization lags or leads similar organizations in cybersecurity maturity, coverage, and performance helps to justify investment and strengthen long-term resiliency against AI risk and other cyber threats.

Final Thoughts

Censinet is an American Hospital Association Preferred Cybersecurity Provider and is purpose-built to help healthcare organizations assess, manage, and mitigate cyber risk.

If you're interested in learning more about how Censinet can help manage AI risk at your organization, contact us at info@censinet.com or visit <https://www.censinet.com>



Censinet is an American Hospital Association Preferred Cybersecurity Service Provider for Cyber Firm Risk Management and Information Governance and Cyber Risk Assessment, Privacy and HIPAA Compliance.