



Healthcare

VANTAGE POINT®

A Healthcare Risk Management Resource | 2025 Issue 2

Artificial Intelligence: A Second Look at an Evolving Technology

Readers of *Vantage Point*® may recall that the publication addressed the issue of artificial intelligence (AI) five years ago, when the concept was first becoming widely familiar. It was then touted as a revolutionary development, which had immense but not fully understood potential in healthcare settings. AI has evolved and continues to evolve on many fronts, transforming clinical processes ranging from diagnostics and medical decision-making to patient/client/resident treatment and care planning.

AI refers to various technologies designed to replicate certain human cognitive functions. (See “Basic AI Terms” on [page 3](#).) Now present in nearly every sector of healthcare, AI can help providers more efficiently analyze complex data, apply findings to clinical situations, render evidence-based treatment decisions and enhance care planning. In fact, according to the McKinsey & Company consulting group, the application of AI-driven algorithms – i.e., sequences of problem-solving instructions working from a defined dataset – and predictive analytics is projected to grow in the health services and technology industry at an average rate of 9 percent annually, reaching \$100 billion in profitability by 2028.

As AI utilization expands within the healthcare industry, so do related liability exposures. This edition of *Vantage Point*® takes a fresh look at AI applications in the healthcare industry, revisits data-related exposures, notes regulatory efforts intended to enhance data quality and minimize bias, and offers an overview of professional liability considerations and associated risk mitigation measures.

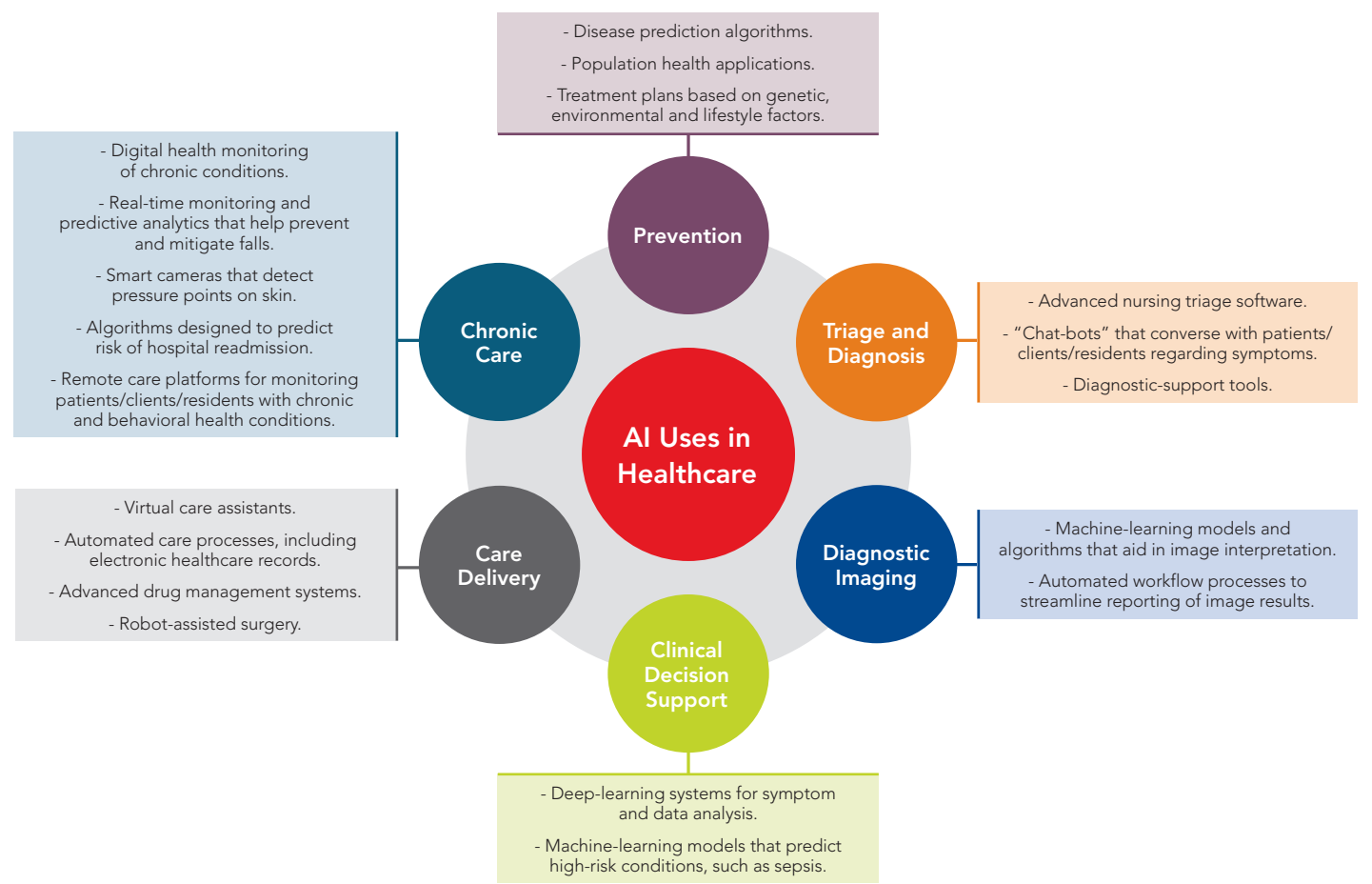
In this issue...

- AI Uses in Healthcare ... [page 2](#).
- Basic AI Terms ... [page 3](#).
- A Note About AI Regulation ... [page 3](#).
- Quick Links ... [page 7](#).

Now present in nearly every sector of healthcare, **AI can help** providers more **efficiently analyze complex data, apply findings** to clinical situations, render **evidence-based treatment** decisions and **enhance care planning**.

Clinical Applications

AI-powered technologies are influencing many clinical, operational and administrative aspects of healthcare. The following diagram suggests the range of current AI tools and applications.



Data-based Risk Exposures

Given AI’s dependence on large quantities of information for training and learning purposes, data integrity arguably constitutes the field’s major vulnerability. The table below displays common data-and process-related risks associated with AI use, along with their implications.

Data Inaccessibility	Data or Outcome Bias	Data Breach	Black-box Reasoning	Automation Bias
Clinical AI tools depend upon the ability to funnel diverse types of information into a single database, which often requires a sophisticated IT infrastructure and a high level of staff expertise.	AI platforms can be undermined by incompatible, inaccurate, obsolete or less-than-inclusive data. Bias may also arise when outdated data fail to reflect changes in patient/client/resident disease patterns or demographics.	AI databases are vulnerable to data breaches and other types of unauthorized disclosures, and require effective security strategies and strictly enforced rules governing access and utilization.	When providers lack full understanding of how an AI algorithm reaches diagnostic or therapeutic conclusions, it can make it more difficult to detect unwanted outcomes and rectify AI system problems.	Excessive trust in automation can erode clinical decision-making skills and encourage complacency, potentially resulting in providers automatically accepting questionable AI-related care recommendations.

Two factors should be kept in mind in regard to data reliability. First, AI models that process and generate human-like text to support clinical decision-making and medical documentation, among other tasks, require “gold standard” data – derived from trusted, expertly curated sources such as MedlinePlus, the U.S. Food and Drug Administration or the PubMed Unified Medical Language System, among others – in order to train machine-learning models. Failure to use reliable benchmark data can lead to incorrect diagnoses, medical errors and other adverse outcomes.

Secondly, datasets should be transparent, with users able to identify the academic or proprietary databases, journal articles or other published materials, clinical guidelines, research findings and other information sources used to train AI systems. Healthcare organizations and providers should conduct due diligence of AI vendors to ensure that the data involved in AI platforms are clean, accurate, up-to-date and extracted from identifiable sources.

Basic AI Terms

Machine Learning

A type of algorithm that reviews data in an iterative manner and reaches a response through statistical analysis, thus enabling software applications to become more useful over time.

Deep Learning

A subset of machine learning involving human-like tasks, such as recognizing speech, analyzing images and rendering diagnoses.

Generative AI

A subset of deep learning that identifies and encodes the patterns and relationships within large amounts of data, then produces “original” content – in the form of text, images or video – to a user’s prompt or request.

Big Data

Massive datasets used for “training” purposes by generative AI programs.

A Note about AI Regulation

At present, there is no comprehensive regulatory framework for medical devices and apps with AI-enabled software functions. The result is a patchwork of rules, as well as gaps and questions that will need to be addressed in the near future. Ongoing regulatory initiatives at the state and federal level focus primarily on the following five areas:

- **Data security and privacy**, to ensure that anonymized data remain protected over the entire lifecycle of an AI model, and that data exported from domestic and global sources are subject to a uniform set of regulations.
- **Data quality**, to guarantee that database sources for AI models and algorithms are accurate, up-to-date and sufficiently representative of the population for which the AI will be used.
- **Algorithm validation**, to verify that machine-learning algorithms can explain how a diagnosis or treatment decision is reached, thus minimizing the “black box” syndrome endemic to AI-based prediction models.
- **Accountability**, to establish clear lines of responsibility for AI-related errors, which can involve AI developers, product suppliers, and/or healthcare providers and organizations, among others.
- **Equitable access**, to ensure that data collection, sharing and usage are governed by ethical principles intended to avoid discrimination and human rights violations, as well as bodily injury to patients/clients/residents.

Healthcare organizations and providers should **conduct due diligence of AI vendors** to ensure that the **data involved** in AI platforms are **clean, accurate, up-to-date** and extracted from **identifiable sources**.

Common Liability Exposures and Risk Mitigation Strategies

Healthcare organizations of all types that currently either use or plan to use AI may wish to consider adopting the risk mitigation strategies listed below, in order to minimize liability exposures.



Implementation and System Training

Liability Exposures	Risk Mitigation Strategies
Inadequate Due Diligence of AI Vendors and Products	• Thoroughly vet AI system vendors, assigning a multidisciplinary team comprising clinical and technical representatives across multiple departments and with varied skill sets. • Evaluate systems prior to purchase, using available assessment checklists. • Select AI systems that offer output interpretation, thus ensuring that clinical decision-making can be easily explained and documented in patient/client/resident healthcare information records. • Test natural language processing software prior to purchase, confirming that it accurately extracts clinical information from a variety of sources, including text, images, and audio and video recordings. • Include clear terms and conditions in vendor contracts concerning such key issues as data privacy and security, regulatory compliance, algorithmic bias and fairness, patient/client/resident safety and efficacy, and liability and indemnification.
Faulty System Implementation	• Draft a robust implementation plan that includes necessary process changes, timelines, training opportunities and performance expectations. • Establish cross-functional teams to collaborate on AI implementation, including data analysts, IT experts and end users. • Pilot-test products with end users, using plausible clinical scenarios, prior to full implementation.
Improper System Training	• Select the “right” data – i.e., datasets that demonstrate variety, volume, veracity and velocity – when training AI systems, remembering that quantity of data by itself does not guarantee quality results. • Adopt AI systems that allow for data exchange across multiple sites, points of service and patient/client/resident populations. • Consult an analytics expert to assist in aggregating data, thus helping ensure more reliable outputs.



Data Quality

Liability Exposures	Risk Mitigation Strategies
Biased Data	• Ensure that AI systems capture a diverse and inclusive range of data, thus reducing potential disparities and inequities. • Include uncommon cases in the data used to train AI systems, in order to expand diagnostic capability. • Maintain records of the data used to train AI systems, including vendor-operated systems. • Retrain AI systems when necessary, e.g., if data bias or other system flaws come to light.
Uncertain Outcomes	• Select AI tools that indicate the extent of confidence or uncertainty about a given clinical output. • Educate users about error-avoidance strategies, using simulated scenarios in which AI decision-support systems produce potentially faulty or uncertain outcomes.



Protocols
and Process

Liability Exposures	Risk Mitigation Strategies
Insufficient Data Governance	• Consult legal counsel and compliance experts when validating AI solutions to ensure they meet regulatory guidelines. • Remain abreast of changing AI standards and regulations at the state and federal level, and update policies and procedures as necessary. • Audit AI-enabled decisions on a regular basis to ensure validity and regulatory compliance.
Failure to Validate the Accuracy of AI	• Create a process for reviewing AI-generated decisions to confirm underlying criteria. • Encourage AI users to validate outputs, thus fostering a culture of accountability. • Train providers to question AI outputs, especially in situations with a low degree of certainty, and to fact-check the system when output decisions are neither simple nor clear.



Staff
Readiness

Liability Exposures	Risk Mitigation Strategies
Inexperienced Users	• Educate users on AI systems, including a comprehensive review of their capabilities and limitations. • Inform users of the protocol for escalating concerns and reporting problems in regard to data integrity and other potential system issues. • Test user proficiency on an annual basis and document the results.
Inappropriate Use of AI	• Develop and enforce clear protocols that govern utilization of AI applications, devices and wearables. • Conduct periodic ethics reviews and assessments of AI cases, in order to identify and address potentially inappropriate utilization of the technology.
Over-reliance on AI	• Inform medical providers about the American Medical Association (AMA) statement regarding “augmented” intelligence, i.e., that AI is designed to complement human decision-making, not to substitute for independent judgment. (See also “Augmented Intelligence Development, Deployment, and Use in Health Care,” issued by the AMA, November 2024.) • Educate users that AI is one tool among others, and that they must apply their professional judgment and critical thinking skills when accepting AI-generated decisions. • Establish mechanisms for human oversight, validation and critical review of AI outputs, in order to track trends and prevent over-reliance.



Clinical Documentation

Liability Exposures Risk Mitigation Strategies

Lack of Informed Consent	• Review and revise informed consent forms to ensure that they address use of AI technology, explain that such systems depend upon a steady flow of patient/client/resident data, and indicate the risk of privacy breaches and invalid or biased conclusions. • Obtain written consent from patients/clients/residents for the use of their anonymized data in training AI algorithms, and explain that they have the right to erase any personal data from AI systems.
Documentation Insufficiencies	• Review how AI decisions are captured in the electronic healthcare record system and, if needed, adopt new documentation standards to enhance the notation of outputs and their supporting rationale. • Require providers to note and describe the influence of AI in making decisions, in order to avoid the appearance of “black-box reasoning” and to help ensure that providers understand and can explain the rationale for AI-influenced decisions.



Security and Risk

Liability Exposures Risk Mitigation Strategies

Data Breaches	• Incorporate effective security measures into AI tools and associated databases, including firewalls, data encryption safeguards and intrusion-detection systems. • Draft permission protocols for sharing and using data from different sources that flow into clinical AI systems. • Conduct regular staff training sessions on cyber security best practices and the importance of safeguarding patient/client/resident data. • Perform routine risk assessments of AI systems and databases to detect potential cyber security threats and devise preventive measures.
Neglecting to Monitor Systems and Report Errors	• Maintain a list of all AI systems and tools utilized in the healthcare setting, as well as their intended application, in order to support user accountability, performance audits and compliance checks. • Monitor AI systems for malfunctions and errors, and respond in accordance with a written protocol. • Routinely track and trend all AI-related incidents that result in patient/client/resident harm, noting whether AI was a primary or contributing factor to the error. • Conduct a root cause analysis of all reported AI errors and implement a corrective action plan, if needed.
Insurance Implications	• Consult legal counsel and insurance company representatives to gauge how AI-enabled technologies may affect the organization’s risk profile and insurance coverage needs. • In the event of lawsuits alleging AI-related error, preserve machine-learning algorithms, so that they may be examined for data validity, presence of bias and compliance with the applicable standard of care.

The above table serves as a reference for healthcare organizations and providers seeking to evaluate risk exposures associated with AI use. The content is not intended to represent a comprehensive listing of all actions needed to address the subject matter, but rather is a means of initiating internal discussion and self-examination. Your organization and risks may be different from those addressed herein, and you may wish to modify the activities and questions noted herein to suit your individual organizational practice and patient/client/resident needs. The information contained herein is not intended to establish any standard of care, or address the circumstances of any specific healthcare organization. It is not intended to serve as legal advice appropriate for any particular factual situations, or to provide an acknowledgement that any given factual situation is covered under any CNA insurance policy. The material presented is not intended to constitute a binding contract. These statements do not constitute a risk management directive from CNA. No organization or individual should act upon this information without appropriate professional advice, including advice of legal counsel, given after a thorough examination of the individual situation, encompassing a review of relevant facts, laws and regulations. CNA assumes no responsibility for the consequences of the use or nonuse of this information.

As the healthcare-related uses of artificial intelligence proliferate, leaders, providers and staff need to be aware not only of AI's ever-widening range of capabilities, but also its inherent limitations and vulnerabilities. By utilizing high-quality data, being aware of possible bias, monitoring AI performance and guarding against over-reliance, healthcare professionals and organizations can reap the benefits of this game-changing technology, while minimizing corresponding risk.

Quick Links

- [Health Care Artificial Intelligence Toolkit](#), issued by the California Telehealth Resource Center, 2024.
- ["Building and Implementing an Artificial Intelligence Action Plan for Health Care,"](#) issued by the American Hospital Association, 2025.

Did someone forward this newsletter to you? If you would like to receive future issues of *Vantage Point*® by email, please register for a complimentary subscription at go.cna.com/HCsubscribe.

Editorial Board Members

Kelly J. Taylor, RN, JD, *Chair*
Nicole Austin, RN, MSN, CPHRM
Janna Bennett, CPHRM
Peter S. Bressoud, CPCU, RPLU, ARE
Elisa Brown, FCAS
Emma Landry
Lauren Motamedinia, J.D.
Michelle O'Neill, MN, MBA, PhD,
CPHRM, CPPS
Karen Schremp-Schinker, MS, BSN,
RN, CCM, CPHRM

Publisher

Patricia Harmon, RN, MM,
CPHRM

Editor

Hugh Iglarsh, MA

For more information, please call us at 888-288-3534 or visit www.nso.com or www.hpso.com.



888-288-3534

www.nso.com

www.hpso.com

The information, examples and suggestions presented in this material have been developed from sources believed to be reliable as of the date they are cited, but they should not be construed as legal or other professional advice. CNA, Aon, Affinity Insurance Services, Inc., NSO, or HPSO accepts no responsibility for the accuracy or completeness of this material and recommends the consultation with competent legal counsel and/or other professional advisors before applying this material in any particular factual situations. This material is for illustrative purposes and is not intended to constitute a contract. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice. Certain coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds. The claims examples are hypothetical situations based on actual matters. Settlement amounts are approximations. Certain facts and identifying characteristics were changed to protect confidentiality and privacy. Any references to non-CNA, non-Aon, AIS, NSO, and HPSO websites are provided solely for convenience, and CNA, Aon, AIS, NSO and HPSO disclaim any responsibility with respect to such websites. "CNA" is a registered trademark of CNA Financial Corporation. Certain CNA Financial Corporation subsidiaries use the "CNA" trademark in connection with insurance underwriting and claims activities. This material is not for further distribution without the express consent of CNA. Copyright © 2025 CNA. All rights reserved. Published 7/25. CNA VP25-2.

Healthcare Providers Service Organization is a registered trade name of Affinity Insurance Services, Inc., a licensed producer in all states (TX 13695); (AR 100106022); in CA, MN, AIS Affinity Insurance Agency, Inc. (CA 0795465); in OK, AIS Affinity Insurance Services, Inc.; in CA, Aon Affinity Insurance Services, Inc., (CA 0G94493), Aon Direct Insurance Administrators and Berkely Insurance Agency and in NY, AIS Affinity Insurance Agency.

Nurses Service Organization is a registered trade name of Affinity Insurance Services, Inc., a licensed producer in all states (TX 13695); (AR 100106022); in CA, MN, AIS Affinity Insurance Agency, Inc. (CA 0795465); in OK, AIS Affinity Insurance Services, Inc.; in CA, Aon Affinity Insurance Services, Inc., (CA 0G94493), Aon Direct Insurance Administrators and Berkely Insurance Agency and in NY, AIS Affinity Insurance Agency.