NHCAA
National Health Care Anti-Fraud Association®

Generative Artificial Intelligence (GenAI) and Health Care Fraud: Opportunities and Mitigation

June 2025

The National Health Care Anti-Fraud Association
1220 L Street NW, Suite 815
Washington, DC 20005
www.nhcaa.org

Acknowledgments

The National Health Care Anti-Fraud Association (NHCAA) extends its sincere thanks to Kurt Spear of Highmark, Inc. for his invaluable support and contributions in developing this issue brief. His expertise, insights, and guidance were instrumental in shaping the final document, and we are deeply grateful for his partnership.

NHCAA also sincerely thanks the AI Work Group, skillfully led by Matthew Berls of UnitedHealthcare and James Bowers of Evernorth Health Services, which envisioned, championed, and directed this issue brief project.

Introduction

Founded in 1985 by several private health insurers and federal and state government officials, the National Health Care Anti-Fraud Association is the leading national organization focused exclusively on the fight against health care fraud and abuse. NHCAA is private-public partnership. Its members comprise private health insurers and those public-sector law enforcement and regulatory agencies having jurisdiction over health care fraud committed against both private payers and public programs.

The NHCAA Mission Statement: "To protect and serve the public interest by increasing awareness and improving the detection, investigation, civil and criminal prosecution, and prevention of health care fraud and abuse."

NHCAA pursues that Mission by:

- Maintaining a strong private-public partnership in combating health care fraud and abuse;
- Providing unparalleled learning opportunities through The NHCAA Institute for Health Care Fraud Prevention;
- Providing opportunities for private- and public-sector information-sharing;
- Serving as a national resource for health care anti-fraud and abuse information and professional assistance to government, industry and the media; and
- Recognizing and advancing professional specialization in the detection and investigation and prosecution of health care fraud through accreditation of health care anti-fraud professionals.

The purpose of this issue brief is to help define Artificial Intelligence (AI) fraud, waste, and abuse (FWA) risks in health care while also creating a mechanism to think through mitigation strategies and opportunities to leverage AI to combat FWA. It is not intended to be a comprehensive or stand-alone document that covers all AI FWA risks or mitigation strategies. This document will continue to evolve as AI and the industry's use of AI matures.

Disclaimer

Any views or opinions expressed in this document are solely those of NHCAA and of the contributing authors and do not necessarily represent those of the contributing authors' respective employers or any NHCAA Member Organization.

Contents

GenAI in Health Care

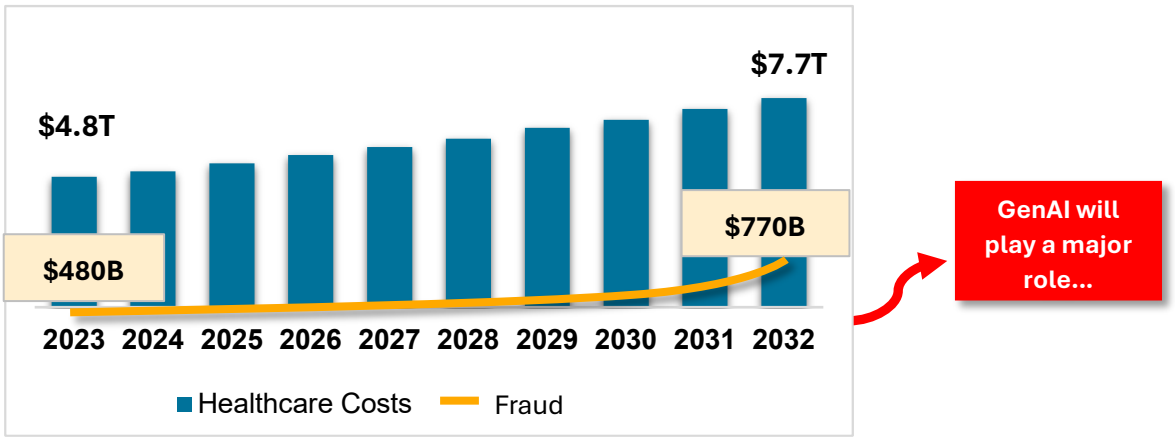
The use of GenAI (defined below) in health care is being enthusiastically pursued as a means to a more efficient, effective, and patient-centered health care system, by addressing:

- Enhanced Patient Care: Increasing face-to-face time may improve patient experience and allow for data-driven, personalized treatment
- Workforce Crisis: Automating administrative tasks may free clinicians to focus more on patient care, reducing burnout and improving efficiency
- Accuracy and Revenue: Reducing human error may lead to better billing, fewer denials, and increased financial stability
- Long-Term Cost Savings: While initial investments may be high, reducing administrative costs and improving efficiency promise significant long-term savings

Increased efficiency, coupled with potential cost savings and improved accuracy, may justify the significant industry investment in GenAI, however, realizing the technology's full potential requires careful consideration of ethical and implementation challenges.

In addition to the benefits that GenAI may offer, it presents significant risks relative to fraud, waste, and abuse ("FWA").

Total health care costs are anticipated to rise from $4.8 trillion in 2023[1] to $7.7 trillion by 2032, while department budgets for Special Investigations Units (SIU) within health insurance plans are often decreasing. It is estimated that anywhere between 3% - 10% of health care expenditures can be attributed to fraud.[2] As the use of GenAI increases, so too will fraud. Plans will need to be incredibly diligent in how funds are dedicated in order to maximize the impact on fraud reduction.



[1] The Centers for Medicare & Medicaid Services, National health expenditure data, Projected, *https://www.cms.gov/data-research/statistics-trends-and-reports/national-health-expenditure-data/projected*

[2] *https://www.nhcaa.org/tools-insights/about-health-care-fraud/the-challenge-of-health-care-fraud/*

A Deeper Look into GenAI

GenAI presents both significant opportunities and considerable risks within the health care industry. Within this brief, we analyze the various ways GenAI can be leveraged to perpetrate fraud, waste and abuse, outlining specific threats and vulnerabilities. Furthermore, we examine the potential of GenAI to enhance FWA detection and prevention, detailing proactive mitigation strategies and outlining a framework for a comprehensive AI-driven approach to combatting health care FWA.

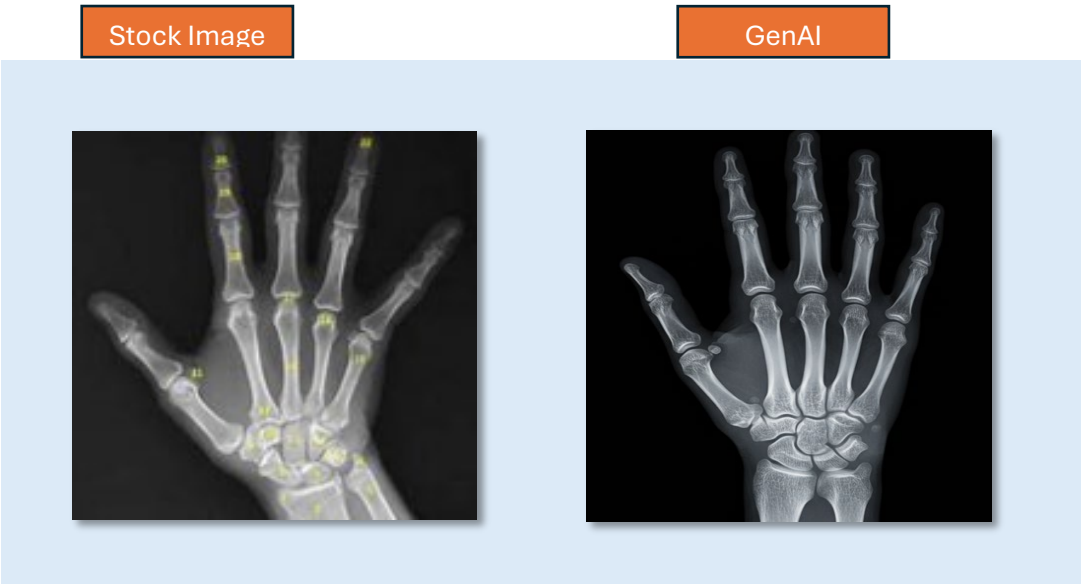
As mentioned above, the health care industry is experiencing a technological transformation driven by the rapid advancements in Artificial Intelligence ("AI"), particularly GenAI. GenAI's ability to generate realistic text, images and audio presents transformative potential for improving efficiency and personalization. However, these same capabilities also pose substantial risks, particularly in the context of FWA. This issue brief aims to provide a comprehensive overview of these dual aspects, offering insights and recommendations for leveraging GenAI's benefits, while effectively mitigating its associated risks.

AI and GenAI Background:

- **Definition of AI:** The National Institute of Standards and Technology ("NIST") defines artificial intelligence or "AI" as "an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations or decisions influencing real or virtual environments." This definition encompasses various AI subfields, including machine learning ("ML"), which enables systems to learn from data without explicit programming.

- **Definition of GenAI:** Generative AI or "GenAI" builds upon ML by learning from existing data to create new, human-like outputs, such as text, images and audio. This capability empowers various applications, but it also introduces a new dimension of risk in fraudulent activities.
- **Evolution of Automation:** This paper traces the progression from basic pattern detection to the sophisticated capabilities of GenAI, highlighting the increasing sophistication of potential fraudulent schemes.

GenAI Risks in Health Care FWA



GenAI significantly enhances the capabilities of fraudsters, increasing the frequency, volume and sophistication of FWA schemes. The technology is easily accessible, inexpensive, and enables users to leverage it to commit fraud without understanding health care. Examples of specific risks include:

- **Increased Volume and Frequency of Existing Schemes:** GenAI can automate the creation of false medical claims, significantly increasing the scale and scope of existing fraudulent activities. Examples include mass-producing bogus claims for Durable Medical Equipment (DME), labs and pharmacies.
- **AI-Powered Fraud Scheme Development:** Fraudsters may leverage GenAI to analyze publicly available insurance policies (medical, reimbursement, etc.), identifying loopholes, ambiguities and weaknesses exploitable for fraudulent claims. Since AI continuously learns from successful and unsuccessful attempts, it can refine its strategies to maximize the likelihood of successful deception and target insurers with the most vulnerable policies.

- **Identity Theft and False Claims:** GenAI can be used to generate realistic fake identities and purchase IDs from the dark web, enabling the creation of untraceable claims.
- **Increased Volume and Frequency of Falsified Authorization Requests and Appeals:** GenAI can generate falsified authorization requests and appeals to facilitate fraud schemes.
- **Creation of Falsified Medical Records:** The use of deepfakes and other GenAI techniques enable the creation of realistic but fabricated medical images and records to support false claims.
- **Impersonation of Clinicians and Regulators:** GenAI can generate realistic text messages, emails and even voice clones to impersonate health care professionals and regulators, facilitating phishing and other deceptive tactics.
- **Impersonation of Members, Enrollees, or Beneficiaries:** GenAI can create realistic text messages, emails, and even voice clones to impersonate members.
- **Impersonation of Employees:** GenAI can generate convincing text messages, emails, and voice clones to mimic employees.
- **Robocalls:** GenAI has the capability to make mass robocalls, impersonating both private and public entities.
- **Unforeseen Risks:** The rapid evolution of GenAI presents the potential for unforeseen and novel fraudulent schemes, highlighting the need for continuous monitoring and adaptation of mitigation strategies.

Opportunities for GenAI in Combatting Health Care FWA

Despite the risks, GenAI offers significant opportunities to enhance the detection and prevention of FWA and to create efficiencies in a space that is often manually intensive:

- **Improved Data Analytics and Risk Scoring:** GenAI can analyze vast datasets to identify patterns and anomalies indicative of fraudulent activity, offering more effective risk scoring and earlier detection. For example, GenAI can analyze medical claims against medical records to determine if timed CPT codes billed on a claim match the times noted within medical records.

- **Automated Case Generation and Referral:** GenAI can automate the process of generating case files and law enforcement referrals, improving efficiency and freeing up human resources.
- **Enhanced Documentation Review:** Machine learning models can review claims, voice and images and identify aberrations for further review, focusing investigators on high-risk areas. GenAI can also be used to identify documents and voice messages created using GenAI.
- **Service Verification Programs**: Implementing automated text messaging to verify services received directly from members can significantly reduce fraudulent claims perpetrated using GenAI.
- **Multi-Source Provider Information Gathering:** AI tools can automate the process of collecting information from multiple sources to assess provider eligibility and identify potentially fraudulent activities.

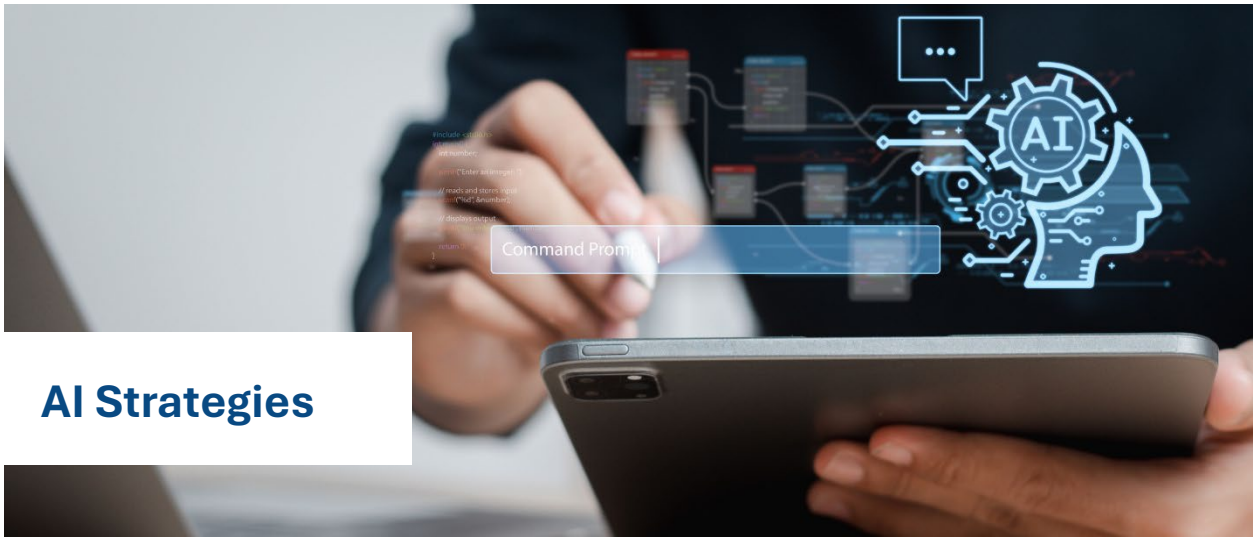
Mitigation Strategies

A multi-faceted approach is needed to effectively mitigate the risks and leverage the benefits of GenAI. GenAI can be a powerful tool for fraud investigators. However, one of the most important attributes to effectively address GenAI-driven fraud is strong investigative capabilities that will help these investigation tools learn, while also ensuring that well-educated humans are at the helm to verify information that comes from these tools. Human oversight for GenAI tools is critically important for many reasons, including, but not limited to, ensuring that GenAI tools aren't built and trained using inaccurate, biased, or otherwise compromised data that provides users with unreliable results.

Key strategies for robust GenAI oversight include:

- **Proactive Contractual Controls:** Incorporating terms and conditions in provider contracts outlining acceptable GenAI use.

- **Verification Techniques:** Implementing robust authentication methods (e.g., watermarks) to ensure the legitimacy of claims, medical records and imaging data.
- **Collaboration and Information Sharing:** Fostering collaboration among health care organizations, government agencies, and technology providers to enhance intelligence sharing that helps educate and combat fraud.
- **Continuous Monitoring and Adaptation:** Maintaining continuous vigilance, regularly updating and adapting mitigation strategies to address emerging GenAI-related threats, and continuing to guard against cyberattacks, corporate espionage, etc.
- **Employee Education and Training:** Providing training across the organization to help recognize and address GenAI-enabled fraudulent tactics (e.g., train claim adjusters on how to look for bogus medical claims created using GenAI), understand prompt engineering, etc.
- **Implementation of AI-Driven Tools:** Leveraging AI tools to enhance risk assessment, fraud detection and case management with fraud investigators at the helm.
- **Ethical Utilization of AI:** Implementing oversight mechanisms to enhance the transparency of AI tools, with regular monitoring to prevent biased decision-making.
- **Public vs. Non-Public AI Tenets:** Providing comprehensive training on the use of public and non-public AI tools, ensuring that protected health information (PHI) and other data consider to be confidential or proprietary remains secure when using public tools.
- **Prompt Engineering and Tuning of AI:** Ensuring the proper engineering of foundational GenAI models and training the models to accurately process and build data models.



AI Strategies

Implementing effective GenAI oversight strategies is essential for improving efficacy and efficiency within the investigative process, both operationally and in the prevention, detection, and remediation of potential fraud, waste, and abuse. As malicious actors are already exploiting GenAI tools, it is crucial to innovate and explore the use of new GenAI technologies, or at the very least, gain a foundational understanding of them. This section outlines key AI strategies, emphasizing responsible AI practices, innovative document scanning tools, verification systems, and risk assessment, including scoring methodologies.

Responsible AI Practices

Collaborate across the enterprise and with external partners to help remain up to date on the rapidly changing landscape of GenAI. For example, work with Procurement and Provider Contracting teams to help ensure agreements outline what can and cannot be performed using GenAI and how tools are developed and used. One critically important control is to ensure that a “human at the helm” approach is utilized. The creation of an AI Governance Committee that includes perspectives of all relevant teams should be considered.

Document Scanning Tools

Innovative tools that automate searching and compiling relevant information on a provider at the initial stage of investigations to enhance risk assignment to focus resource allocation on high risk, high return activities.

Service Verification

This system will send text messages to members with claims flagged for risk factors (e.g., unknown provider TIN, high-risk procedures, state-mandated random sample, etc.). Non-responsive members or members responding that they did not receive a stated service will trigger a "claim net," halting payments pending review. The anticipated outcome is faster fraud detection, reduced overpayments and improved member satisfaction.

Risk Assessment and Scoring Methodology

A risk assessment scores fraud/abuse investigations based on Impact/Exposure (financial and patient impact) and Urgency (care quality or adverse consequences). High scores trigger escalation to enterprise leadership; lower scores do not. A matrix visually represents the scoring and should follow the path of a member's journey from enrollment to claims payment.

Conclusion

GenAI presents a complex challenge for the health care industry. While offering substantial opportunities across health care, including opportunities to combat FWA, it simultaneously enhances the capabilities of fraudsters. A proactive, comprehensive strategy encompassing contractual controls, advanced verification techniques, inter-organizational collaboration, continuous monitoring, and the implementation of innovative and effective AI-driven tools is essential.

The health care industry must embrace a risk-based approach, prioritizing resources toward high-risk, high-return activities. Balancing the continuous monitoring and adaptation required for the evolving landscape of GenAI with the oversight of subject matter experts from across disciplines using a "human at the helm" approach is critical to maintaining the integrity of the health care system.