

Artificial Intelligence and Health Care Fraud:

Evolution from Theory to Reality to the New Normal

NATIONAL HEALTH CARE ANTI-FRAUD ASSOCIATION

October 2026

Acknowledgments

This issue brief reflects the collective insight of health care anti-fraud professionals, investigators, and public- and private-sector partners who are working to understand and respond to the rapidly evolving role of artificial intelligence in fraud, waste, and abuse. Their contributions help ensure the document remains practical, balanced, and focused on protecting members, patients, payers, providers, and public programs.

Executive Summary

Artificial intelligence (AI) is rapidly changing the health care fraud, waste, and abuse (FWA) landscape. It is becoming part of both the threat landscape and the solution set. AI can help bad actors create synthetic identities, falsified records, convincing impersonations, fabricated claim narratives, and scalable appeals or authorization requests.

At the same time, responsible AI can help anti-fraud teams improve risk scoring, review large volumes of unstructured data, identify anomalies, verify services, create administrative efficiencies, and prioritize investigative resources.

- **The threat is immediate and scalable:** AI lowers the barrier to creating convincing false documentation, communications, identities, and utilization patterns.
- **The opportunity is equally significant:** AI can help investigators surface patterns earlier, focus on higher-risk activity, and make better use of claims, unstructured clinical, provider, and member data.
- **Governance is essential:** AI tools should be explainable, auditable, monitored, and supported by clear policies for acceptable use, data protection, model performance, and escalation.
- **Human judgment remains central:** AI can identify risk and accelerate review, but trained investigators must evaluate evidence, apply professional judgement, determine whether AI was used appropriately or with the intent to mislead, and engage with all vested parties involved in a FWA case.

The central challenge is not whether AI will affect FWA work, it already does, but whether anti-fraud organizations can leverage AI more effectively and at a greater pace than the schemes they are trying to stop.

Table of Contents

Introduction.....	5
AI in Health Care	6
AI Background	7
AI Risks in Health Care FWA.....	8
Opportunities for AI in Combatting Health Care FWA.....	11
Mitigation Strategies	13
Responsible AI Practices.....	14
AI Case Study	14
Conclusion	16
Helpful Tools & Links.....	17

Introduction

Founded in 1985 by private health insurers and federal and state government officials, the National Health Care Anti-Fraud Association (NHCAA) is a leading national organization focused exclusively on combating health care fraud and abuse. NHCAA operates as a private-public partnership whose members include private health insurers and public-sector law enforcement and regulatory agencies with jurisdiction over health care fraud involving 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 to combat health care fraud and abuse;
- Providing learning opportunities through The NHCAA Institute for Health Care Fraud Prevention;
- Creating opportunities for private- and public-sector information sharing;
- Serving as a national resource for health care anti-fraud information and professional assistance to government, industry, and the media; and
- Recognizing and advancing professional specialization in the detection, investigation, and prosecution of health care fraud through accreditation of health care anti-fraud professionals.

This updated issue brief defines emerging artificial intelligence (AI) risks related to health care fraud, waste, and abuse (FWA) and outlines practical opportunities to use AI responsibly in anti-fraud programs. The brief is intended to help anti-fraud leaders and work groups align on common terminology, recognize how bad actors may exploit AI, and identify mitigation strategies that combine advanced analytics with strong investigative judgment. It is not exhaustive; it is designed to evolve as AI capabilities, fraud schemes, regulatory expectations, and industry practices continue to change.

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.

AI in Health Care

- **Enhanced Patient Care:** Increasing face-to-face time may improve patient experience and support more data-driven, personalized treatment.
- **Workforce Relief:** Automating administrative tasks may allow clinicians to focus more on patient care, reduce burnout, and improve efficiency.
- **Accuracy and Revenue Integrity:** Reducing human error may support more accurate billing, fewer denials, and greater financial stability.
- **Long-Term Cost Savings:** Although initial investments may be high, reducing administrative costs and improving efficiency may create meaningful long-term savings.

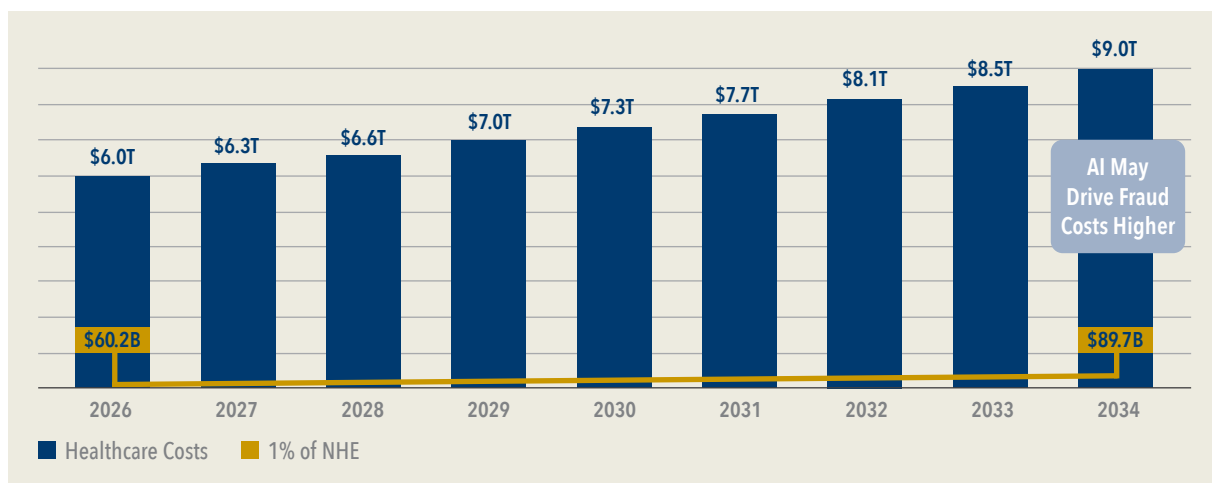
These potential benefits may justify continued investment in AI. However, time will tell if the use of AI is driving efficiency or creating more checks and balances in an already complex system. As providers deploy AI to help promote productivity and revenue optimization, payers and regulators are deploying AI to assess care delivery and the appropriateness of payment of those services. Realizing AI's full value requires careful governance, clear accountability, human oversight, and rigorous evaluation of ethical, operational, privacy, and implementation risks.

The same capabilities that create operational value also introduce significant FWA risk. AI can increase the speed, scale, and believability of fraudulent activity, making it essential for payers and partners to modernize detection, verification, and investigative approaches.

The financial stakes are substantial. CMS projected national health expenditures of \$6.0 trillion for 2026¹, rising to \$9.0 trillion by 2034. Against spending of that scale, even a small rate of fraud—say one percent—translates into enormous losses. NHCAA estimates that health care fraud costs tens of billions of dollars each year, and other industry estimates run higher still.

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>

NATIONAL HEALTH EXPENDITURE (NHE) PROJECTIONS



Source: CMS, Office of the Actuary

Because successful fraud is by definition undetected, the true figure is difficult to measure, but its impact on the health care system is unquestionably significant. As AI becomes more embedded in anti-fraud work, programs will need to direct their limited resources with greater precision, focusing investment on the high-risk, high-impact opportunities for prevention, detection, and recovery.

AI presents a dual reality for the health care industry. It can help anti-fraud programs work faster and smarter, while also giving bad actors new tools to create, disguise, and scale fraudulent activity. This brief examines both sides of that reality such as how AI may be used to perpetrate FWA and how responsible AI strategies can strengthen prevention, detection, investigation, and remediation.

AI can generate realistic text, images, audio, video, summaries, code, and synthetic content. These capabilities create opportunities to improve efficiency and decision support, but they also make fraudulent materials more convincing and easier to produce at scale. For anti-fraud leaders, the priority is to understand where AI changes the risk profile and where responsible AI can create administrative efficiencies and improve investigative outcomes without replacing human judgment.

AI Background

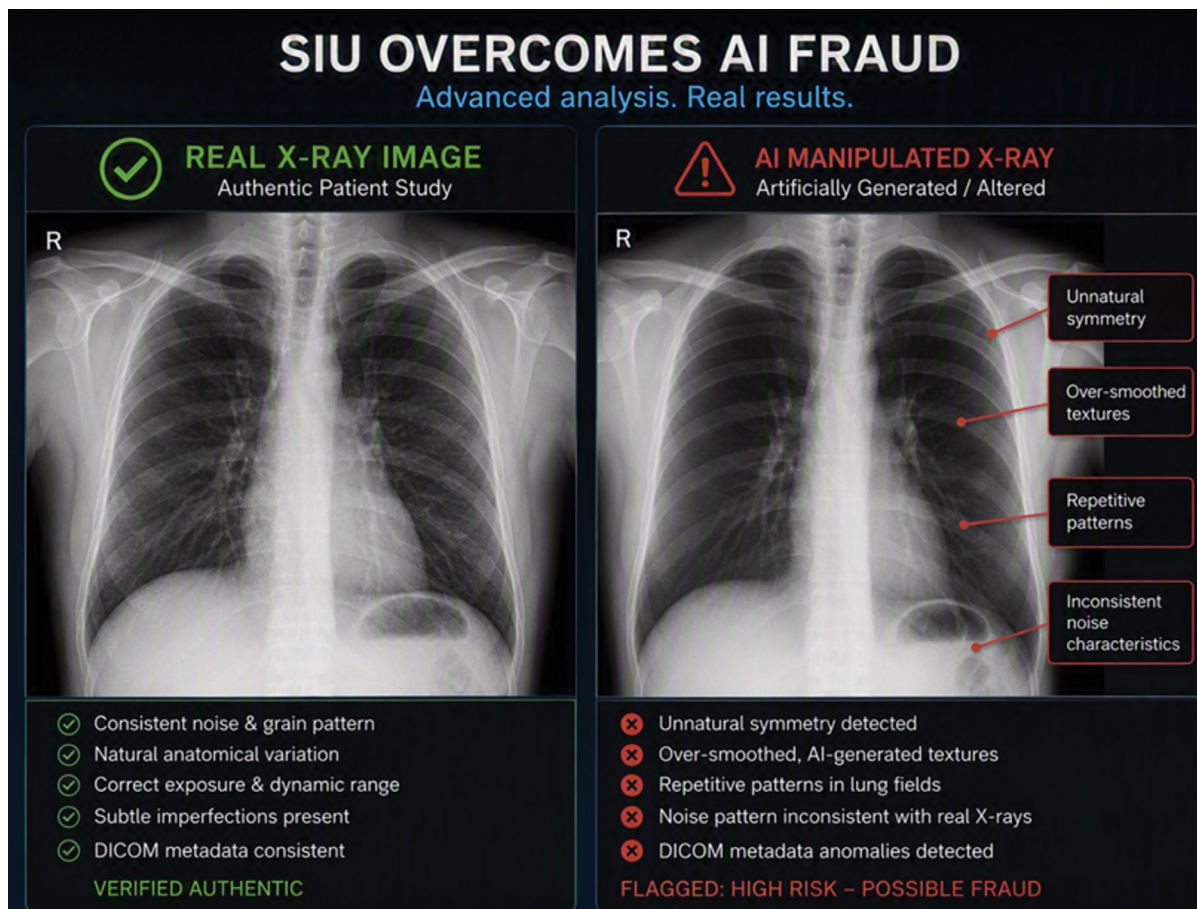
- **Definition of AI:** The National Institute of Standards and Technology (NIST) defines artificial intelligence or “AI” as “an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations or decisions influencing real or virtual environments.” 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.
- **Definition of Agentic AI:** Agentic AI can autonomously plan, make decisions, take actions, and adapt to changing circumstances in pursuit of defined goals, operating with greater independence compared to traditional AI systems.
- **Evolution of Automation:** This paper traces the progression from basic pattern detection to the sophisticated capabilities of AI, highlighting the increasing sophistication of potential fraudulent schemes.

AI Risks in Health Care FWA

AI can increase the volume, speed, and sophistication of FWA schemes. It is widely accessible, relatively inexpensive, and can help users create convincing content without deep knowledge of health care operations, clinical documentation, coding, billing rules, or payer policies. Key risk areas 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 activity. Examples include mass-producing bogus claims for durable medical equipment, labs, and pharmacy services.
- **AI-powered fraud scheme development:** Fraud actors may use AI to analyze publicly available insurance policies, reimbursement rules, and medical policies to identify loopholes, ambiguities, and weaknesses that can be exploited for fraudulent claims.
- **The potential for patient harm from the use of AI in schemes:** The use of AI to create medical documentation or substitute for a qualified clinician may result in significant patient harm due to false or incorrect diagnoses, inaccurate treatment plans, and medical treatment based on AI generated information.
 - One example of potential patient harm includes an AI generated treatment plan for a patient who has been enrolled in a hospice program when it is not medically necessary (the patient does not meet the hospice criteria). Not only can the patient no longer receive curative care, but the AI generated plan may indicate “Do Not Resuscitate” or “Do Not Call 911” when that is not appropriate for the patient (and the patient does not have a Living Will indicating such).
 - Another example is an AI generated false claim for diabetic supplies that incorrectly indicates a diabetes diagnosis. The patient could receive incorrect or harmful medical care if this incorrect diagnosis is included in the electronic health record – especially in emergency situations where the patient is not conscious.
- **Identity theft and false claims:** GenAI can be used to generate realistic fake identities and enable the creation of difficult-to-trace claims.



- **Falsified authorization requests and appeals:** GenAI can generate persuasive but false authorization requests and appeals to support fraudulent schemes.
- **Creation of falsified medical records:** Deepfakes and other GenAI techniques can enable realistic but fabricated medical images and records to support false claims.
- **Impersonation of clinicians and regulators:** GenAI can generate realistic messages, emails, and voice clones to impersonate health care professionals and regulators.
- **Impersonation of members, enrollees, or beneficiaries:** GenAI can create realistic messages, emails, and voice clones to impersonate members and support social engineering or false service verification.

- **Synthetic Identities: Building Phantom Profiles:** The foundation of many advanced fraud schemes is the synthetic identity. Phantom profiles are fabricated persona built by combining stolen data fragments with AI-generated details. Because the identity is not tied to a single real person, it can be difficult to trace and validate. AI can quickly and accurately locate and compile proprietary, personally identifiable, and protected health information from disparate sources to create patient or provider identity portfolios for false billing. These identities may include sensitive data such as Social Security numbers, especially those belonging to individuals whose information may be less actively monitored. GenAI can then create plausible addresses, contact information, employment histories, and superficial digital footprints to help the identity appear authentic during verification checks.
- **Impersonation of employees:** GenAI can generate convincing messages, emails, and voice clones to mimic employees and support phishing, social engineering, or unauthorized access attempts.
- **Robocalls:** GenAI can support mass robocalls that impersonate private or public entities and increase the reach of fraudulent outreach.
- **Unforeseen risks:** The rapid evolution of GenAI may create novel fraudulent schemes, reinforcing the need for continuous monitoring and adaptive mitigation strategies.
- **Plausible Service Utilization Patterns:** By analyzing real claims data, AI models can learn service patterns associated with specific conditions and generate claim sequences that appear legitimate. For example, a fabricated injury could be paired with a realistic sequence of consultations, imaging, therapy, and prescription claims using plausible billing codes.
- **Deepfake Impersonations in a Telehealth World:** Perhaps one of the most alarming developments is the use of deepfake technology to create hyper-realistic video and audio for impersonation of clinicians.
 - **Patient Impersonation:** In the age of telehealth, fraudsters can use a real-time deep-fake video of a “patient” in a virtual consultation with a real clinician. This “digital puppet” can be used to exaggerate or completely fabricate symptoms to obtain legitimate prescriptions or justify fraudulent disability claims. These real-time deepfakes can often bypass basic biometric and liveness checks, making them a potent tool for identity fraud.
 - **Provider Impersonation:** Scammers can clone a doctor’s voice to call in fake prescriptions to a pharmacy or use a deepfake video of a reputable physician to lend credibility to a fraudulent scheme. Bad actors can use just a few seconds of an audio clip of a person’s voice, often obtained from public sources like interviews or presentations, to create a convincing vocal clone. This is used for “vishing” (voice phishing) attacks to authorize prescriptions for controlled substances or trick staff into revealing sensitive patient data.
- **Data Poisoning:** Fraud actors are likely to develop more sophisticated AI-enabled documentation, voice, video, and data manipulation tactics. A particularly concerning frontier is data poisoning. Fraudsters intentionally introduce misleading information to degrade detection models or train them to overlook specific patterns of fraud.

Opportunities for AI in Combatting Health Care FWA

Despite these risks, AI can materially strengthen FWA prevention and investigation when it is governed, explainable, auditable, and paired with experienced human review. High-value opportunities include:

- **Improved data analytics and risk scoring:** AI can analyze large datasets to identify patterns and anomalies that may indicate fraud, supporting more effective risk scoring and earlier detection.
- **Predictive Analytics for Proactive Prevention:** Instead of detecting fraud only after it occurs, AI models can assess the likelihood of fraud before a claim is paid. By comparing incoming claims against known fraudulent behaviors, predictive analytics can assign a risk score to a claim, provider, or patient. High-risk claims can be flagged for human review, helping prevent losses before payment. This feature is also effective for screening new providers requesting enrollment.
- **Natural Language Processing (NLP) for Unstructured Data Analysis:** A significant portion of crucial medical information is locked away in unstructured text, such as clinical notes, pathology reports, and patient correspondence. Natural Language Processing (NLP) allows AI systems to read and analyze this text to identify inconsistencies that may indicate fraud. This allows more claims and medical records to be assessed with greater consistency and accuracy. Examples include looking for diagnoses and severity that don't follow care pathways.
- **Faster Triage of Potential FWA Complaints:** Public and private agencies frequently manage a high volume of complaints from various stakeholders including members, caregivers, and providers. While a significant portion of these inquiries pertain to coverage matters, others are related to potential FWA concerns. Integrating human-in-the-loop AI tools for complaint screening and triage can enhance the operational effectiveness and efficiency of investigative/compliance units.
- **Identifying Specific Fraud Types:** These NLP tools can automatically flag inconsistencies to identify various fraud schemes. For example, they can detect upcoding by flagging a discrepancy between a note describing "mild hypertension" and an insurance claim that bills for "severe hypertension". Overutilization is quickly recognized by performing frequency analysis on notes to find providers billing for an excessive number of procedures in a short time. They can also spot unbundling by comparing service descriptions in the notes with billing codes to see if procedures that should be bundled are billed separately.
- **Cross-Referencing and Anomaly Detection:** NLP can cross-reference information across a patient's entire record to flag claims inconsistent with their known medical history. Partnering with clinically trained professionals is more important than ever when evaluating claims for possible FWA. Infusing greater clinical detail within analytics goes well beyond assessing billing or coding anomalies, pattern detection by looking for diagnoses, treatments, and prescription drugs that are not aligned with acceptable care pathways. Unsupervised learning techniques can then identify outliers and anomalies in the textual data of claims.

- **Detecting Audio and Visual Deepfakes:**

- **Audio Forensics:** Detection systems use voice biometrics to create a “voiceprint” by analyzing unique vocal characteristics like pitch and cadence. They also analyze audio waveforms for subtle artifacts and distortions introduced during synthesis, using techniques like Zero Crossing Rate (ZCR) to spot alterations. Multi-modal analysis cross-references audio with video to detect mismatches between lip movements and spoken words.
- **Visual Forensics:** Advanced deep learning models like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are trained on vast datasets to spot fakes. These tools scrutinize media for tell-tale signs like unnatural eye movements, mismatched lip-syncing, irregular skin textures, blending glitches, and temporal inconsistencies between video frames. Frequency domain analysis can also reveal anomalies that are not visible to the naked eye.
- **Liveness Detection:** As a first line of defense in telehealth, liveness detection verifies a user is real. Active methods require the user to perform an action like blinking, while passive methods work in the background, analyzing cues like skin texture and light reflections.
- **Automated Case Generation and Referral:** AI can automate the process of generating case files and law enforcement referrals, improving efficiency, and enabling more effective allocation of investigative resources.
- **Enhanced Documentation Review:** Machine learning models can review claims, voice recordings, and images to identify aberrations for further review, allowing investigators to focus on high-risk areas.
- **Service Verification Programs:** Implementing automated text messaging to verify services rendered to patients 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. Information gathering on suspect actors can be collected in minutes instead of hours.
 - Innovative tools can automate searching and compiling relevant information on a provider at the initial stage of investigations to enhance risk assignments to focus resource allocation on high risk, high return activities.

The future of fraud mitigation will require transparent, adaptive AI systems supported by vigilant human oversight and robust verification protocols. Explainability is essential: investigators, legal teams, regulators, and law enforcement partners must be able to understand, test, reproduce, and defend AI-assisted outputs. A black-box model can create risk if its reasoning cannot be explained or reproduced.

A multi-faceted approach is needed to effectively mitigate the risks and leverage the benefits of AI. AI can be a powerful tool for fraud investigators. However, one of the most important attributes to effectively addressing AI-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 AI tools is critically important for many reasons, including, but not limited to, ensuring that AI tools aren't built and trained using inaccurate, biased, or otherwise compromised data that provides users with unreliable results.

Mitigation Strategies

Key strategies for robust AI oversight include:

- **Proactive contractual controls:** Incorporate terms and conditions in provider contracts that define acceptable AI use, documentation expectations, audit rights, and accountability for misuse.
- **Verification techniques:** Implement robust authentication methods, such as provenance markers and watermarking, to help validate claims, records, images, and related documentation.
- **Collaboration and information sharing:** Foster collaboration among health care organizations, government agencies, law enforcement, and technology partners to improve threat intelligence and mitigation strategies.
- **Continuous monitoring and adaptation:** Regularly update strategies, controls, and detection models to address emerging threats and related cyber, privacy, and corporate espionage risks.
- **Employee education and training:** Train employees to recognize GenAI-enabled tactics, protect sensitive data, understand approved AI use, and escalate suspicious activity appropriately. Employees should also be trained in how AI tools work and evolve to help understand their capabilities.
- **Implementation of AI-driven tools:** Use AI tools to enhance risk assessment, fraud detection, documentation review, case management, and administrative tasks, while keeping investigators accountable for final determinations.
- **Ethical use of AI:** Implement oversight mechanisms to improve transparency, reduce bias, monitor model performance, and support defensible decision-making.
- **Public and non-public AI use:** Provide guidance on approved AI tools and ensure protected health information, confidential information, and proprietary data are not entered into unapproved public tools.
- **Prompt engineering and model tuning:** Use disciplined prompt design, model testing, tuning, and validation to improve accuracy, consistency, and reliability.

Effective AI oversight is essential to improving anti-fraud efficacy and efficiency. Because many malicious actors are already using AI tools, anti-fraud organizations should develop a practical understanding of AI capabilities, risks, and controls. This section outlines strategies that emphasize responsible AI governance, document review automation, verification systems, service validation, and risk-based scoring.

Responsible AI Practices

Collaborate across the enterprise and with external partners to help remain up to date on the rapidly changing landscape of AI. For example, work with Procurement and Provider Contracting teams to help ensure agreements outline what can and cannot be performed using AI 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.

AI Case Study

A healthcare fraud scheme often begins when criminals obtain stolen personal health information through data breaches, cyberattacks, or illicit online marketplaces. Rather than immediately using the information, they frequently target dormant identities, such as individuals who rarely use healthcare services, because fraudulent activity is less likely to be detected quickly. Using artificial intelligence, fraudsters then enrich these stolen identities with information gathered from social media, public records, and other online sources, creating realistic digital personas that appear legitimate.

Once these synthetic identities are established, fraudsters leverage generative AI to rapidly create large volumes of healthcare claims. Technology enables them to produce claims that appear authentic while varying the details enough to avoid obvious duplication. To maximize their chances of success, claims are often submitted during weekends, holidays, or other periods when payer organizations may have reduced staffing and oversight. The volume and sophistication of these submissions can overwhelm traditional detection methods, allowing some fraudulent claims to proceed through adjudication and payment.

As suspicious billing patterns begin to emerge, Special Investigations Units (SIUs) step in to validate the legitimacy of the claims. Investigators request supporting medical records and documentation to confirm that services were rendered and that the clinical information supports the billed charges. However, AI has also enhanced the fraudster’s ability to respond to scrutiny. Generative AI can create convincing medical records, laboratory reports, medical images, and professional-looking appeal letters that contain realistic clinical narratives and supporting documentation designed to withstand manual review.

To combat these increasingly sophisticated schemes, SIUs are turning to AI-powered investigative tools. Investigators analyze document metadata, examine digital artifacts, review image characteristics, and compare records across large datasets to identify signs of cloning, fabrication, or AI generation. Advanced analytics help uncover hidden patterns, duplicated content, subtle inconsistencies, and anomalies that would be difficult or time-consuming for a human reviewer to detect independently. Through a combination of investigative expertise and technology, SIUs can distinguish legitimate documentation from synthetic content and build evidence to support fraud determinations and recovery efforts.

Ultimately, the fraud lifecycle becomes an ongoing race between increasingly sophisticated criminals and increasingly capable investigators. As fraudsters continue to adopt AI to scale and automate their schemes, healthcare SIUs must continuously evolve their detection strategies, leveraging AI not only to identify fraudulent claims and cloned records, but also to stay ahead of emerging threats and protect the integrity of the healthcare system.

AI ON BOTH SIDES OF THE FIGHT

AI is used to commit healthcare fraud. SIU uses AI to detect, investigate, and prevent it.

HOW FRAUDSTERS USE AI

To commit healthcare fraud



1. CREATE FALSE IDENTITIES

AI generates synthetic identities, fake provider profiles, and stolen patient information at scale.



2. GENERATE FRAUDULENT CLAIMS

AI creates upcoded, unbundled, or medically unnecessary claims that mimic legitimate patterns to evade rule-based edits.



3. BUILD FAKE NETWORKS

AI maps and creates shell entities, kickback networks, and phantom referral chains to conceal relationships.



4. MANIPULATE & DECEIVE

AI-powered chatbots coach patients and providers on how to falsify documentation and evade detection.



5. EVOLVE & ADAPT

AI continuously learns from edits, denials, and audits to adapt schemes and stay ahead of detection.



THE SAME
AI CAPABILITIES
CAN BE USED
FOR HARM
OR FOR
PROTECTION.



HOW SIU USES AI

To detect, investigate, & prevent fraud

1. ADVANCED RISK DETECTION

AI analyzes vast amounts of structured and unstructured data to identify suspicious providers, claims, and beneficiaries in real time.



2. PATTERN & ANOMALY IDENTIFICATION

Machine learning detects complex patterns and anomalies humans and rule-based systems miss—even in low-frequency fraud.



3. NETWORK & LINK ANALYSIS

AI uncovers hidden relationships, common owners, circular referrals, and financial connections behind fraudulent schemes.



4. INTELLIGENT INVESTIGATION SUPPORT

AI prioritizes cases, summarizes evidence, extracts key facts from documents, and speeds investigator productivity.



5. PREVENTION & CONTINUOUS LEARNING

AI models learn from outcomes, investigations, and emerging trends to strengthen controls and prevent future fraud.



STRONGER DETECTION

Find more fraud, earlier.



FASTER INVESTIGATIONS

Focus on what matters most.



HIGHER RECOVERIES

Stop losses and recover more dollars.



SAFER HEALTHCARE

Protect patients, providers, and the integrity of care.

AI WON'T REPLACE FRAUD INVESTIGATORS.
BUT FRAUD INVESTIGATORS WHO USE AI WILL REPLACE THOSE WHO DON'T.

Conclusion

AI presents a defining challenge for health care anti-fraud programs. It can improve detection, documentation review, service verification, and investigative prioritization; it can also help fraud actors create more convincing identities, records, communications, and claim patterns at scale. The organizations best positioned to adapt will be those that treat AI as both a strategic opportunity and a controlled risk.

A practical path forward requires risk-based investment, strong governance, explainable tools, continuous monitoring, collaboration across public and private partners, and a disciplined “human at the helm” model. AI can help investigators surface patterns, prioritize leads, and accelerate review, but it cannot prove intent. That responsibility remains with trained investigators who can evaluate evidence, context, and credibility.

Helpful Tools & Links

BROAD STATE AI LEGISLATION AND GOVERNANCE

National Conference of State Legislatures (NCSL) - Artificial Intelligence Legislation Database

A broad, searchable database of introduced and enacted state AI legislation. Its subject filters include AI in health care, government use, private-sector use, responsible use, and discrimination, making it a strong starting point for monitoring the state-law landscape.

Access: NCSL AI Legislation Database

<https://www.ncsl.org/financial-services/artificial-intelligence-legislation-database>

MultiState - Artificial Intelligence Legislation Tracker

Tracks AI-related legislation across all 50 states through an interactive map. Users can filter bills by state, legislative chamber, status, and topic, making the tool useful for identifying proposed and enacted measures that may affect health-care delivery, insurance operations, payment integrity, or fraud investigations.

Access: MultiState – State AI Legislation Tracker

<https://www.multistate.ai/artificial-intelligence-ai-legislation>

International Association of Privacy Professionals (IAPP) - U.S. State AI Governance Legislation Tracker

Tracks cross-sector state AI governance bills affecting private organizations, including automated decision-making, risk assessments, transparency, discrimination, and developer/deployer duties. It is especially useful for identifying horizontal rules that may reach insurers, providers, vendors, or fraud-analytics programs.

Access: IAPP U.S. State AI Tracker

<https://iapp.org/resources/article/us-state-ai-governance-legislation-tracker>

Epstein Becker Green - State AI Law Tracker

Continuously updated map of enacted state AI laws, organized into omnibus, health care and life sciences, and employment categories. The health-care category highlights requirements affecting coverage decisions, clinical uses, disclosure, human oversight, and nondiscrimination.

Access: EBG State AI Law Tracker

<https://www.ebglaw.com/insights/publications/state-ai-law-tracker>

Steptoe – AI Legislative Tracker

Monitors proposed and enacted AI legislation at both the federal and state levels. The tracker provides bill summaries, sponsors, current status, and direct links to full legislative text. It is a useful complement to state-focused resources because it allows readers to follow congressional activity and compare it with emerging state requirements.

Access: Steptoe – AI Legislative Tracker

<https://www.steptoe.com/en/ai-legislative-tracker.html>

HEALTH CARE-SPECIFIC AI POLICY

Anti-fraud lens. Track rules that enable AI in care delivery and administration alongside rules governing investigative, payment-integrity, coverage, and enforcement uses. Permissions and constraints may not develop in parallel.

Manatt Health - Health AI Policy Tracker

Focuses on federal and state AI developments in health care. It is particularly useful for tracking payor use of AI, prior authorization, medical necessity, clinical oversight, disclosures, governance, and regulatory sandboxes.

Access: Manatt Health AI Policy Tracker

<https://www.manatt.com/insights/newsletters/health-highlights/manatt-health-health-ai-policy-tracker>

Holland & Knight - State AI Health Tracker

Interactive state map covering laws affecting health insurers, health care providers, digital health, and health privacy. It provides short summaries and legal citations and can be filtered to isolate health-insurance measures relevant to claims, utilization review, and fraud detection.

Access: Holland & Knight State AI Health Tracker

<https://view.ceros.com/holland-and-knight/state-ai-health-tracker/p/1>

Public Citizen - State Legislation Regulating AI in Healthcare Coverage Decisions

A focused tracker of enacted, pending, failed, vetoed, and withdrawn state bills addressing AI in health-insurance coverage decisions. Its narrow scope makes it a useful supplement for monitoring human-review, transparency, and limits on automated adverse determinations.

Access: Public Citizen Coverage-Decision Tracker

<https://www.citizen.org/article/tracker-state-legislation-regulating-use-of-ai-in-healthcare-coverage-decisions/>

Kaiser Family Foundation (KFF) – AI, Claims Review, and Program-Integrity Analysis.

KFF publishes timely analyses of AI in prior authorization, claims review, billing, and health-care delivery, including federal and state consumer protections. Its work is especially useful for understanding how policies enabling provider and insurer AI may create new fraud risks while imposing different constraints on coverage, payment-integrity, and investigative uses. KFF also maintains a separate tracker of federal and state Medicaid program-integrity activity.

Access: KFF – Regulation of AI in Prior Authorization and Claims Review

<https://www.kff.org/patient-consumer-protections/regulation-of-ai-in-prior-authorization-and-claims-review-a-look-at-federal-and-state-consumer-protections/>

Access: KFF – Medicaid Program Integrity Tracker

<https://www.kff.org/medicaid/medicaid-program-integrity-tracking-state-specific-and-nationwide-federal-action/>

INSURANCE REGULATION AND SUPERVISORY ACTIVITY

National Association of Insurance Commissioners (NAIC) - Artificial Intelligence Resources

The central source for state insurance regulators' AI principles, model guidance, and supervisory activity. The Model Bulletin materials show the state-by-state regulatory patchwork, while the AI Working Group covers oversight of insurer AI used in claims, fraud detection, underwriting, pricing, and utilization management.

Access: NAIC AI Topic Page

<https://content.naic.org/insurance-topics/artificial-intelligence>

Access: Model Bulletin Adoption Map

<https://content.naic.org/sites/default/files/legal-adoption-map-ai-model-bulletin.pdf>

Access: NAIC AI Working Group

<https://content.naic.org/committees/h/big-data-artificial-intelligence-wg>

FEDERAL HEALTH CARE PROGRAM INTEGRITY

Centers for Medicare & Medicaid Services (CMS) - Center for Program Integrity

The primary CMS source for Medicare, Medicaid, and Marketplace program-integrity priorities, guidance, reports, and initiatives. CMS expressly identifies AI and predictive analytics as tools for reducing fraud, waste, and abuse.

Access: CMS Center for Program Integrity

<https://www.cms.gov/medicare/medicaid-coordination/center-program-integrity>

CMS - Fraud, Waste & Abuse Hub

A central publication point for CMS fraud priorities, reports, dashboards, enrollment actions, and medical-review initiatives. Important AI-enabled activity may appear here as an operational initiative rather than as an AI rule.

Access: CMS Fraud, Waste & Abuse Hub

<https://www.cms.gov/fraud>

U.S. Department of Health and Human Services, Office of Inspector General (HHS-OIG)

Provides the OIG Work Plan, audits, evaluations, enforcement actions, and reports concerning HHS programs. These materials reveal both oversight of federal AI governance and the risks and controls associated with analytics in program integrity.

Access: HHS-OIG

<https://www.oig.hhs.gov/>

U.S. Government Accountability Office (GAO)

GAO reports examine how CMS and other agencies use analytics to detect and prevent fraud, often providing operational detail not visible in legal texts. Its 2026 Medicare fraud report illustrates the intersection of AI-enabled fraud and government analytics.

Access: *GAO Medicare Data Analytics Report*

<https://files.gao.gov/reports/GAO-26-107799/index.html>

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.