2024

Balancing the Scales: Harnessing the Power of Artificial Intelligence (AI) in Healthcare Fraud Detection While Navigating AI's Perils

Ally Winter

I. Introduction

The healthcare industry has long been regarded as one of the broadest and most rapidly advancing fields in the world. Sub-sectors within the realm of "healthcare" include healthcare services and facilities, medical devices, pharmaceuticals, and health insurance. From stem cell therapies and laparoscopic surgeries to nursing homes and pediatricians, everyone has had delicate and personal experiences with healthcare providers and services at some point. Saturated with consistent innovation and advancement, a primary goal of the healthcare field is to ceaselessly learn and develop; but, such knowledge and development comes at a cost. In 2020 alone, the total health care expenditure (hereinafter "HCE")[1] in the United States totaled $4.1 trillion.[2] This staggering number accounts for approximately 45% of the $9 trillion (USD) spent on HCEs *globally* in 2020.[3]

Parallel to the consistent growth of the healthcare field is the consistent growth of healthcare fraud. The National Health Care Anti-Fraud Association (NHCAA) estimates that 3% of the United States' annual HCEs, totaling $300 billion *at minimum*, are lost to healthcare fraud each year.[4] Other government and law enforcement agencies speculate that the number could be as high as 10% of the United States' annual HCEs.[5] In an effort to mitigate the amount wasted on fraud each

[1] *See* Centers for Disease Control and Prevention, Health Care Expenditures (last reviewed June 26, 2023), https://www.cdc.gov/nchs/hus/topics/health-care-expenditures.htm#refl (defining health care expenditure as "represent[ing] the amount spent on health care and related activities such as private and public health insurance, health research, and public health activities").
[2] Apoorva Rama, *Policy Research Perspectives: National Health Expenditures, 2020: Spending Accelerates Due to Spike in Federal Government Expenditures Related to the COVID-19 Pandemic*, American Medical Association (2022), https://www.ama-assn.org/system/files/prp-annual-spending-2020.pdf (last visited Nov. 22, 2023).
[3] *Global spending on health: rising to the pandemic's challenges*, Geneva: World Health Organization (2022), https://www.who.int/publications/i/item/9789240064911 (last visited Nov. 24, 2023).
[4] *The Challenge of Health Care Fraud*, National Health Care Anti-Fraud Association, https://www.nhcaa.org/tools-insights/about-health-care-fraud/the-challenge-of-health-care-fraud/ (last visited Nov. 22, 2023).
[5] *Id.*

year, Congress has implemented acts such as the False Claims Act (FCA)[6] and the Anti-Kickback Statute (AKS)[7] which monitor and limit physicians' billing and referral capabilities.[8]

Recently, artificial intelligence (hereinafter "AI")[9] has begun to transform the way that many people live their lives and conduct their business. From personal organization to autonomous vehicles and facial recognition systems, AI has allowed us to see a glimpse into the future as it steadily advances – advances that have swiftly made their way into healthcare and are utilized both administratively and medically.[10]

There are many potential benefits to the continued implementation of AI in healthcare fraud detection. AI systems may be programmed to process data sets and detect anomalies indicating fraudulent practices. Large amounts of data may be processed and dissected in short amounts of time and can adapt to rules and procedures as they are programmed into the system to uncover fraud before the human eye could or would. For example, a system can be trained to review specific billing claims and determine whether the services billed for were appropriate considering the patient's individual diagnosis and medical history, and the physician's billing codes.[11] As the healthcare industry continues to grapple with the financial burden of fraudulent activities, the integration of AI technologies offers a compelling solution.

However, as we venture further into the realm of AI in healthcare fraud detection, a look to the dangers posed by AI in other contexts piques interest. General risks associated with the use

---

[6] 31 *U.S.C.* §§ 3729-3733.
[7] 42 *U.S.C.* § 1320a-7b(b).
[8] *See infra*, Section II, Subsection B, and accompanying text for definition and further explanation.
[9] *See infra*, Section III and accompanying text for definition and further explanation.
[10] *See infra*, Section III and accompanying text for an in-depth discussion on the different applications of AI in the healthcare sector.
[11] Vicki Hyman, *Diagnosis: Fraud. How AI can detect scams in healthcare*, www.mastercard.com (June 28, 2021), https://www.mastercard.com/news/perspectives/2021/how-ai-can-detect-scams-in-healthcare/.

of AI include bias and discrimination, and security and privacy concerns.[12] For example, COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) – a commercial risk assessment algorithm used to predict the recidivism risk of those incarcerated – was found to be inappropriately flagging black and male defendants as having a 63.2% higher risk of re-offending when compared to white and female defendants.[13] Though plagued with bias unknowingly engrained into its decision-making process, this algorithm is utilized to determine parole and probation eligibility of those incarcerated.[14] Thus, exposing individuals to the biased algorithm may have detrimental effects on whether or not they are deemed eligible for release.

Another potential risk associated with AI is that there is not currently any federal legislation in place governing its use. This absence allows individuals the freedom to create algorithms, use and store data, and publish or sell their systems without any guidance or oversight. Promulgating AI regulation could make AI safer overall and could begin to mitigate the existential risks that AI poses to fueling discrimination and misinformation; but, before calling for regulation to promote AI's continued use in healthcare fraud detection specifically, one must be sure that the same risks apply.

Whether or not these risks should influence AI's use exclusively in healthcare fraud requires a careful analysis of the specifically applicable risks. This paper begins in Section II with a general introduction to healthcare fraud and abuse, describing the federal statutes designed to prevent such fraud and moving into the many ways the government detects healthcare fraud currently. Section III then introduces AI and its overall history and benefits. AI's use in healthcare

[12] Bernard Marr, *The 15 Biggest Risks of Artificial Intelligence,* Forbes (Jun. 2, 2023, 03:07 AM), https://www.forbes.com/sites/bernardmarr/2023/06/02/the-15-biggest-risks-of-artificial-intelligence/?sh=2040e1892706.
[13] Jeff Larson, et al., *How We Analyzed the COMPAS Recidivism Algorithm,* ProPublica (May 23, 2016), https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.
[14] *Id.*

fraud specifically is then detailed, followed by an overview of the risks of AI both generally and specifically to healthcare fraud detection. It ends with a brief description of the nonexistent state of federal AI regulations. Section IV then weighs all the potential risks of AI's continued use and analyzes whether lingering concerns should result in change.

II. Understanding Healthcare Fraud and Abuse: Background

A general understanding of healthcare fraud and abuse is required to properly consider whether AI is a fitting solution to the problem. This section begins with an introduction to the many forms of healthcare fraud and abuse and moves into the various federal statutes in place to prevent it. It ends with a discussion of the traditional ways that the government has been fighting fraud prior to and following AI's implementation.

A. What is Healthcare Fraud and Abuse?

The first documented account of healthcare "fraud" comes from the 19th-century phenomenon of railway spine: a controversial disease presenting as "microscopic changes to the spine that could not be seen."[15] As the alleged result of frequent railway collisions, railway spine found itself to be the leading cause of action in personal injury lawsuits, typically resulting in insurance settlements at the hands of opportunistic plaintiffs. This spectacle laid the foundation for the definition and management of fraud, specifically in the insurance industry.

The definition of fraud has continuously evolved and is now defined by the Health Insurance Portability and Accountability Act (HIPAA) as when one "knowingly, and willfully executes or attempts to execute a scheme … to defraud any healthcare benefit program or to obtain by means of false or fraudulent pretenses, representations, or promises any of the money or property owned

[15] Ken Dornstein, *Accidentally, On Purpose: The Making of a Personal Injury Underworld in America*, St. Martin's Press, 1996.

by … any healthcare benefit program."[16] In layman's terms, healthcare fraud is the intentional deception, misrepresentation, or concealment of information to receive unauthorized benefits or payments from government-funded healthcare programs. Abuse is a broader term, and the difference between fraud and abuse varies based on the circumstance, intent, and knowledge of the individual. Primarily, abuse "describes [provider's] practices that may directly or indirectly result in unnecessary costs to the Medicare Program" and fail to meet the professionally recognized standards within the industry.[17]

Actions that constitute healthcare fraud and abuse include, but are not limited to, kickbacks and billing fraud. Kickbacks are defined by the Center for Medicare & Medicaid Services (hereinafter "CMS") "as offering, soliciting, paying, or receiving remuneration (in kind or in cash) to induce, or in return for the referral of patients or the generation of business involving any item or service for which payment may be made under Federal healthcare programs."[18] For example, it is prohibited for a physician to accept payment from a lab in exchange for referring patients as this constitutes a kickback. While not illegal in *all* industries, kickbacks involving federal healthcare programs are expressly prohibited as they can result in overutilization and unfair competition.[19]

Billing fraud is more complex because there are a few different types. Underneath the wide umbrella of billing fraud is billing for unnecessary services,[20] billing for services or items not actually performed or furnished (phantom billing), submitting multiple claims for the same service

[16] Health Insurance Portability and Accountability Act. Pub. L. No. 104-191, § 264, 110 Stat.1936
[17] Hossein Joudaki, et al., *Using Data Mining to Detect Health Care Fraud and Abuse: A Review of Literature*, Glob J. Health Sci. 7(1) 194-202 (Aug. 31, 2014), https://doi.org/10.5539/gjhs.v7n1p194.
[18] *Common Types of Health Care Fraud* (July 2016), Centers for Medicare & Medicaid Services, https://www.cms.gov/files/document/overviewfwacommonfraudtypesfactsheet072616pdf (last visited Dec. 1, 2023).
[19] *See infra* for discussion of Anti-Kickback Statute in Section II, Subsection B.
[20] Per the Social Security Act § 1902(a)(30)(A), States are required to "provide such methods and procedures relating to the utilization of, and the payment for, care and services available under the plan ... as may be necessary to safeguard against unnecessary utilization of such care and services."

(double billing), upcoding,[21] and unbundling.[22] These fraud schemes are most commonly executed by physicians and providers who perform services for patients and subsequently bill government-sponsored healthcare programs for said services as opposed to private health insurance providers.

B. Federal Healthcare Fraud Statutes

Regulations play an important role in our society in that they promote fairness and efficiency. They set standards and mandate compliance with an approved set of rules to ensure that entities within a given industry are on an even playing field. The healthcare industry is no different, and regulatory entities that produce and enforce regulations to combat healthcare fraud specifically include the Office of Inspector General (OIG), the Department of Justice (DOJ), and CMS. The three most important rules promulgated by Congress and regulated by those agencies for our purposes are the False Claims Act (hereinafter "FCA"), the Anti-Kickback Statute (hereinafter "AKS"), and the Physician Self-Referral Law (hereinafter "Stark Law").

The FCA makes it illegal to submit claims or cause a claim to be submitted for payment to either Medicare or Medicaid that a provider *knows* or *should know* are false or fraudulent.[23] This includes submitting a claim for payment to Medicare for a blood test that was knowingly never performed. The FCA imposes both civil and criminal penalties for violations.

---

[21] Though not defined specifically in any regulation, upcoding is generally understood to mean billing for services at a more complex level than the service *actually* provided or documented in the file. U.S. Department of Health and Human Services, Office of Inspector General, *Testimony of Inspector General Daniel Levinson Before the House Appropriations Committee, Subcommittee on Labor, Health and Human Services, Education, and Related Agencies* (Mar. 4, 2010, 01:15 PM), https://oig.hhs.gov/newsroom/testimony/efforts-combat-health-care-fraud-waste-and-abuse-medicare-and-medicaid/.

[22] According to the Federal Bureau of Investigation, unbundling "is the practice of submitting bills in a fragmented fashion in order to maximize the reimbursement for various tests or procedures that are required to be billed together at a reduced cost." Federal Bureau of Investigation, *Financial Crimes Report to the Public: 2010-2011*, http://www.fbi.gov/stats- services/publications/financial-crimes-report-2010-2011. An example would be a provider billing and entering a code for both the incision and the suturing that occurs in a surgical procedure, rather than using a standard billing code that encompasses both. This differs from phantom billing, where a provider deliberately submits a bill for payment knowing that no medical service was actually provided.

[23] 31 U.S.C. §§ 3729-3733.

The AKS is a criminal law that prohibits the knowing or willful payment, offer, solicitation, or receipt of remuneration to induce or reward patient referrals or the generation of business involving any service or item payable by a federal healthcare program.[24] Remuneration includes anything of value but is not limited to merely cash. For example, providing expensive meals and hotel stays can qualify as remuneration under the AKS. Unlike the FCA, an individual's intent is an important aspect of their liability under the AKS. Penalties for AKS violations include fines, imprisonment, and exclusion from participation in any Federal healthcare program.

The Stark Law prohibits individuals from referring patients to receive "designated health services" from entities with which the physician or an immediate family member has a financial relationship when said services are payable by Medicare or Medicaid, absent an exception.[25] "Designated health services" include therapy services, home health services, prescription drugs, and both inpatient and outpatient hospital services. Violations of the Stark Law constitute a strict liability offense, meaning no reference to the individual's intent is required. Penalties for a Stark Law violation can include fines and exclusion from participation in any Federal healthcare program.

Additionally, HIPAA specifically establishes healthcare fraud as a federal criminal offense subject to extensive fines and up to 10 years in prison.[26] Any fraudulent activity that results in injury to or death of a patient can double the maximum prison sentence to 20 years or result in a life sentence in federal prison, respectively. HIPAA also specifically establishes a national Health Care Fraud and Abuse Control Program (HCFAC), under the joint direction of the Attorney General and the Secretary of the Department of Health and Human Services (HHS) acting through

[24] 42 U.S.C. § 1320a-7b(b).
[25] 42 U.S.C. § 1395nn.
[26] 18 U.S.C. § 1347.

the Department's Inspector General (HHS/OIG). This program aims to combat fraud by mandating the cooperative enforcement efforts of federal, state, and local law enforcement officers against healthcare fraud.

C. Traditional Ways That the Government Has Been Detecting Healthcare Fraud

The fight against healthcare fraud cannot be done alone. In addition to the regulatory bodies that are charged with enforcing the aforementioned regulations, government agencies partner together and employ an array of strategies to uncover and combat fraudulent practices.

Traditionally, Medicare and Medicaid fraud has been detected by utilizing data to physically conduct audits without the assistance of computers or software. For example, Section 1936 of the Social Security Act (42 U.S.C. 1320a-7c(a)(2)) created the Medicaid Integrity Program (MIP), which obligates CMS to hire contractors – called Audit Medicaid Integrity Contractors (Audit MICs) – to conduct post-payment audits on Medicaid claims.[27] These Audit MICs are required to review what items or services are furnished by providers under State plans,[28] audit claims for payment, and identify overpayments.[29] Following their audit, the Audit MIC must prepare a draft audit report and submit it to CMS, who then reviews and finalizes the report, specifies any identified overpayments, and submits it to the state. The state then pursues the collection of any overpayment according to state law.[30] Other contractors hired by CMS to prevent,

---

[27] *Fact Sheet: National Medicaid Audit Program* (Nov. 2012), Medicaid Integrity Program, https://www.cms.gov/medicare-medicaid-coordination/fraud-prevention/provider-audits/downloads/mip-audit-fact-sheet.pdf (last visited Nov. 25, 2023).

[28] A State health insurance plan is one that is funded and run by the federal government. They include Medicare, Medicaid, and CHIP – each requiring an applicant to meet differing qualifying criteria including surpassing a specific age or having a disability. Individuals may also elect to purchase private health insurance which is a contract between the individual and the private company. Private health insurance can be purchased directly from the insurance company, through an employer, or through the Affordable Care Act's marketplace. Lena Borrelli, *What is Private Health Insurance?* Forbes (Dec. 1, 2023, 08:41 AM), https://www.forbes.com/advisor/health-insurance/private-health-insurance/#:~:text=A%20private%20health%20plan—including,such%20as%20Medicaid%20and%20Medicare (last visited Dec 3, 2023).

[29] *Id.*

[30] *Id.*

detect, and investigate fraud include Comprehensive Error Rate Testing (CERT) Contractors, Medicare Administrative Contractors (MAC), and Unified Program Integrity Contractors (UPIC).

Other government anti-fraud and abuse partnerships include the Healthcare Fraud Prevention Partnership (HFPP) and the Healthcare Fraud Prevention and Enforcement Action Team (HEAT). HFPP, created by Section 1128C(a)(2) of the Social Security Act (42 U.S.C. 1320a-7c(a)(2)), is a private-public partnership that aims to detect and prevent fraud by creating a platform for HFPP partners to collaborate and share data and information.[31] HEAT was independently established by the DOJ, OIG, and HHS to enhance existing programs combatting fraud and expand the DOJ-HHS Medicare Fraud Strike Force, which targets criminal fraud schemes.[32]

Though seemingly straightforward, healthcare fraud is an increasingly complex and difficult problem. As the methods of battling fraud change and broaden with time, so do the mechanisms of conducting fraud. Continuous technological and intellectual advancements including AI make it easier for agencies to uncover the schemes as they occur. Thus, in 2011, CMS launched the Fraud Prevention System (FPS) which used data analytics to identify unusual and suspicious billing patterns in Medicare claims prior to payment.[33] This program was CMS' first glimpse of AI and machine learning's possibilities of uncovering healthcare fraud.[34]

---

[31] *See Healthcare Fraud Prevention Partnership: About the Partnership*, Centers for Medicare & Medicaid Services, https://www.cms.gov/medicare/medicaid-coordination/healthcare-fraud-prevention-partnership/about (last visited Dec. 3, 2023).

[32] *Medicare Fraud & Abuse: Prevent, Detect, Report*, Centers for Medicare & Medicaid Services, https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/Fraud-Abuse-MLN4649244.pdf (last visited Dec. 3, 2023).

[33] *Report to Congress: Fraud Prevention System, Second Implementation Year, June 2014*, Centers for Medicare & Medicaid Services, https://www.cms.gov/About-CMS/Components/CPI/Widgets/Fraud_Prevention_System_2ndYear.pdf (last visited Dec. 3, 2023).

[34] It is important to note the difference between data analytics and artificial intelligence, as the two are intrinsically intertwined but different. Data analytics operates by using data sets to detect historical patterns and anticipate future events. Artificial intelligence implements data analysis but uses sophisticated software to go one step further and formulate sophisticated predictions and assumptions like the thought processes of a human brain.

III. Understanding Data Analytics and AI for Healthcare Fraud

To fully consider the question of whether AI's general risks apply to healthcare fraud and whether regulation will prove any benefit, one must understand AI generally and its slow implementation in healthcare fraud detection. This section begins with an introduction to AI's history and moves into the different types of AI used for healthcare fraud detection. The various types of AI currently utilized in healthcare fraud detection are then discussed, followed by an in-depth examination of the risks of AI and the lack of existing regulation.

A. Background and Benefits of AI

Artificial intelligence is "the capability of computer systems or algorithms to imitate intelligent human behavior."[35] It is not one singular type of technology, but rather a body of them. Put simply, it is the simulation of human intelligence and mental ability by machines that are programmed to "think" and "act" like humans. These machines are built to process and analyze vast amounts of data quickly, learn from said data, and make informed decisions and predictions based on their learning – essentially mirroring the internal decision-making process of a human. To better understand AI's complexities, a look back at its development is necessary.

The history and growth of artificial intelligence are a testament to the remarkable evolution of human and scientific innovation. The concept of AI was first hinted at in 1939 in *The Wizard of Oz*'s heartless Tin Man and brainless Scarecrow. While these individuals moved and spoke like humans, they knew they lacked the key ingredient to truly *being* human and believed that the Wizard was the only one who could save them. Lucky for them, in 1950, the real-life wizard of AI, Alan Turing, published the first literature contemplating the creation of an intelligent, human-

[35] *Artificial intelligence*, MERRIAM-WEBSTER DICTIONARY ONLINE, https://www.merriam-webster.com/dictionary/artificial%20intelligence.

like machine.[36] But, these machines seemed impossible at the time due to their cost and the overall state of underdeveloped computerized technology. This all changed in 1956 when the Dartmouth College Artificial Intelligence Conference officially coined the term "artificial intelligence" and introduced the first AI program, the "Logic Theorist."[37] This program was designed to mimic a human's mathematical problem-solving skills by utilizing manually input mathematical theorems and performing automated reasoning.[38] Organizer John McCarthy stated that the purpose of this conference was "to proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it," and AI was officially born.[39]

Following this conference, in 1959, IBM's Arthur Samuel popularized the term "machine learning" (ML) following his creation of the Samuel Checkers-Playing computer learning Program.[40] ML is a subset of AI, and its systems utilize programmed algorithms to analyze input data sets and "learn" from them in the same way a human would.[41] Samuel's program improved in skill the more it played by studying which moves resulted in game wins and incorporating those moves into its algorithm.[42]

The success of this knowledge-driven approach led to the creation of the data-driven approach in the 1990s, which allowed programs to analyze large sets of data and additionally formulate

---

[36] Alan Turing, *Computing Machinery, and Intelligence* (1950).
[37] Rockwell Anyoha, *The History of Artificial Intelligence*, Harvard Medical School, Science in the News Blog: Special Edition on Artificial Intelligence (Aug. 28, 2017), https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/.
[38] *Id.*
[39] *Artificial Intelligence Coined at Dartmouth*, Dartmouth College, https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth (last visited Dec. 3, 2023).
[40] Arthur L. Samuel, *Some Studies in Machine Learning Using the Game of Checkers*, 3 IBM Journal of Research and Development 535 (1959).
[41] *What is machine learning?* Internal Business Machines, https://www.ibm.com/topics/machine-learning (last visited Dec. 3, 2023).
[42] *See Samuel*, *supra* note 40.

conclusions and knowledge based on the results.[43] These advancements have led to AI's infiltration in nearly all aspects of our lives. From the movies that Netflix recommends to a simple Google search, most of our associations with technology have underlying algorithms and AI technologies powering them.

B. AI for Healthcare Fraud Generally

Throughout the 1900s as AI and ML continued to develop, fraud detection was performed solely by rule-based systems which use predefined rules to flag potentially fraudulent claims based on specific criteria.[44] These systems employ data mining, which is the process of combing through data sets to identify different patterns and anomalies. These predefined rules are manually input by humans based on expert knowledge and research, and include specifications such as account number, amount, location, frequency, and time stamps.[45] Once data sets are uploaded, the system serves as a gatekeeper and flags claims based on what rules they do or do not satisfy.[46] Rule-based systems rely on solely human intervention to perform quality checks on and update the rules as time goes on. This requires more time and money as they must be continuously monitored and updated to adapt to new threats and schemes.[47] Additionally, this method of fraud detection is costly as it requires constant review by experts and auditors expected to review all seemingly fraudulent claims.

---

[43] Bernard Marr, *A Short History of Machine Learning – Every Manager Should Read,* Forbes (Feb. 19, 2016, 02:31 AM), https://www.forbes.com/sites/bernardmarr/2016/02/19/a-short-history-of-machine-learning-every-manager-should-read/?sh=398262be15e7.

[44] *Rule-Based Fraud Detection,* Fraud.net, https://fraud.net/d/rules-based-fraud-detection/#:~:text=Algorithmic%20fraud%20detection%2C%20better%20known,systems%20do%20this%20work%20automatically (last visited Dec. 3, 2023).

[45] *Id.*

[46] *Bridging the Gap: Incorporating AI/ML into Rules-Based Fraud Detection Models,* Fraud.net, https://fraud.net/n/bridging-the-gap-incorporating-ai-ml-into-rules-based-fraud-detection-models/ (last visited Dec. 3, 2023).

[47] *Id.*

Though rule-based systems were the traditional way to detect fraud, the continuing advancement of data-driven AI systems makes them valuable and paramount to knowledge-driven AI. Given the increasing complexity and rise of healthcare data along with the proliferation of electronic medical records (EMRs), data-driven AI can be perfectly tailored to uncover specific fraudulent activity and billing practices and continually learn and apply new knowledge in the process. The increased use of computerized technology within the healthcare industry can make it easier to extract specific knowledge from a wide set of health insurance claims and differentiate a subset of claims that appear to the system to be fraudulent or abusive.[48]

At the core of all fraud-detecting AI systems are data sets. For a system to detect fraudulent practices, the system must be educated on what typically is or is not fraudulent and must have sets of data to comb through in order to learn. These data sets, called fraud classification data sets, are derived from aggregated data sets made publicly available by CMS. On their website, CMS breaks the data sets up into "Programs," "Provider & Care Types," "Geography," and "Topics." Within "Topics" is "Health Care Use & Payments," which then breaks the data sets down even further into various categories including "Medicare Physician & Other Practitioners – by Provider" and "Medicare Durable Medical Equipment, Devices & Supplies – by Referring Provider and Service."

These data are collected in a de-identified manner to ensure anonymity.[49] As data sets may differ in structure based on insurer and specific purpose, the data sets must then be "cleaned" and

[48] *See Joudaki, supra* note 17.

[49] De-identification involves stripping sensitive data of its identifiers, which include an individual's name, address, birth date, demographic information, and medical history. Section 164.514(a) of the HIPAA Privacy Rule states that health information is considered "not individually identifiable if it does not identify an individual and if the covered entity has no reasonable basis to believe it can be used to identify an individual." *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule,* U.S. Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Dec. 3, 2023).

preprocessed before being loaded into the system and run through an algorithm.[50] Cleaning data includes "merging years of data, normalizing columns, imputing missing values, transforming values, reconciling inconsistencies, feature selection, and removing duplicate entries."[51]

Data-driven AI methods can be broken down into three types: supervised, unsupervised and hybrid learning. Supervised learning methods utilize knowingly fraudulent and legitimate transactions and compare them to newly input data sets to identify fraud and train the algorithm for future use. For fraud specifically, all supervised learning methods are the same in that they all contain "a labeled dataset (i.e., fraudulent: yes or no), a domain-specific justification to choose one algorithm versus another, and a performance metric of choice to determine the best algorithm."[52] This form of learning is intrinsically dependent upon the accuracy of the labeled data set used to dissect and categorize the new data sets.

Unsupervised learning methods review data sets and identify patterns or structures based on an algorithm. They are used when there are no labels within the data sets for the algorithm to actively learn from and are merely organizational. It is often referred to as "outlier detection," and is frequently used to identify fraud specifically as it can decide whether different sets of data relate or vary from one another.[53] Hybrid learning methods combine both supervised and unsupervised learning but use each technique at different stages. Multiple algorithms are used together to complement and enhance each other, solving intricate problems that each individual algorithm would be unable to solve alone.

---

[50] Justin M. Johnson and Taghi M. Khoshgoftaar, *Data-Centric AI for Healthcare Fraud Detection*, Springer Nature Computer Science 4(4), 389 (May 11, 2023), https://doi.org/10.1007/s42979-023-01809-x.
[51] *Id.*
[52] Nishamathi Kumaraswamy, et al., *Healthcare Fraud Data Mining Methods: A Look Back and Look Ahead*, Perspect Health Information Management 19(1), 1i (Jan. 1, 2022), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9013219/#B84.
[53] *Id.*

C. Application of AI in Healthcare Fraud Detection

As AI is an obvious and seemingly perfect fit for use in healthcare fraud detection, it comes as no surprise that it is already being implemented. A 2020 report conducted by New York University and Stanford researchers for the Administrative Conference of the United States uncovered that 45% of federal agencies surveyed were already using ML and/or AI.[54] Of these federal agencies using AI/ML are the Department of Health and Human Services (HHS) and CMS. The HHS Chief Information Officer Karl Mathias stated during an AFCEA Bethesda Health IT event on January 16, 2023, that DHS was launching a pilot program to utilize tree-based AI models to detect Medicare fraud, in connection with CMS.[55] Tree-based AI is exactly as it sounds – a decision tree resemblant of a flowchart is made based off of a data set to predict a target value using if-then rules. After seeing "some" success, Mathias intended to keep growing the program.[56] No other information could be found regarding the program or its effectiveness.

In 2011, CMS launched its Fraud Prevention System (FPS) which utilizes predictive analytics and ML to analyze claims data and evaluate fraud both before and after payment is made. FPS can likewise identify provider-specific suspicious billing practices to create investigatory leads and deny individual payment claims that the system flags as fraudulent. CMS estimates that FPS has helped to "prevent or identify nearly $1.5 billion in improper and potentially fraudulent payments from its implementation [in 2011] through the end of the calendar year 2015."[57] In addition to FPS, CMS has expressed its interest in the continued use of AI, dedicating a website to

---

[54] David Freeman, et al., *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies*, Administrative Conference of the United States (Feb. 2020), https://reglab.stanford.edu/publications/government-by-algorithm/.
[55] Nihal Krishan, *HHS CIO Mathias says tree-based AI models helping to combat Medicare fraud,* FedScoop (Jan. 18, 2023), https://fedscoop.com/hhs-cio-mathias-says-tree-based-ai-models-helping-to-combat-medicare-fraud/.
[56] *Id.*
[57] *Medicare: CMS Fraud prevention System Uses Claims Analysis to Address Fraud*, U.S. Government Accountability Office (Aug. 30, 2017), https://www.gao.gov/products/gao-17-710.

it that documents its intended future use of the systems and the resources it offers its employees who are interested in it.[58]

Given the simplicity and independence of AI technologies, large companies within the private sector have also started to take advantage of the market for systems specific to healthcare fraud detection. For example, Alaffia Health is a private company retailing pre-programmed AI systems, called LeverageAI, geared specifically toward uncovering healthcare fraud. They advertise that they directly serve "payers," namely health plans, third party administrators, reinsurers, and government agencies, to "proactively prevent overpayments" and "stay ahead of the curve."[59] LeverageAI is able to perform bill and claim reviews as well as claims editing, and contains an "Ask Autodor" AI assistant that is "tailor-made to help you instantly summarize medical records, source clinical guidelines, and draft determination responses."[60]

Alaffia is not the only private company retailing these technologies. Mastercard's Brighterion similarly markets AI healthcare fraud detection systems to "payers," and notes that it uses both AI and ML (unsupervised and supervised learning) to do so.[61] H20.ai markets fraud detection systems to financial services, healthcare, insurance, manufacturing, marketing and retail customers, including Nationwide Auto Insurance and PayPal.[62] Highmark approaches AI systems from a different angle and incentivizes its services as an insurance provider by providing additional

[58] *Artificial Intelligence at CMS*, Centers for Medicare and Medicaid Services, https://ai.cms.gov (last visited Dec. 3, 2023).
[59] *Who We Serve*, Alaffia Health, https://www.alaffiahealth.com/who-we-serve/health-plans (last visited Dec. 3, 2023).
[60] *Our Solutions*, Alaffia Health, https://www.alaffiahealth.com/our-solutions (last visited Dec. 3, 2023).
[61] *Healthcare Fraud, Waste and Abuse*, Mastercard Healthcare Solutions, https://brighterion.com/healthcare-ai-reduce-fwa/ (last visited Dec. 3, 2023).
[62] *Case Studies*, H2O.ai, https://h2o.ai/case-studies/ (last visited Dec. 3, 2023).

AI systems for both healthcare fraud detection ("cost management") and assistance with clinical diagnoses ("care management") to "improve the Employee Health Experience."[63]

The benefits and possibilities of utilizing AI for healthcare fraud detection to both the government and private companies are seemingly endless. These include faster processing time, larger processing capability, and less labor costs. Nonetheless, nothing good comes easy, and there are risks associated with AI's use.

D. Risks Associated with AI Generally

All success comes with drawbacks, and AI is no exception. Using AI in any context poses significant risks due to its vast capabilities. These risks primarily include bias and discrimination, and data security and privacy. When thinking of bias, one typically thinks of racism and sexism – human biases. While human, these biases often get subconsciously baked into the algorithms used for AI and have been found to produce skewed results. Bias in an algorithm exists when said algorithm makes erroneous or incorrect assumptions resulting in systemically prejudiced results based on a bias unknowingly built into or learned by the system.[64] For example, a study testing a hospital algorithm able to predict which patients will most likely need follow-up care following their visit discovered that the algorithm classified white patients as over 25% sicker than black patients.[65] Of the 46% of black patients who actually needed follow-up care, the bias that was engrained into the algorithm permitted the system to identify only 18% – an algorithm that was based entirely on patients' raw insurance claims data.[66] A Stanford study similarly identified racial

---

[63] *AI and Data Analytics Improve the Employee Health Experience,* Highmark, https://www.highmark.com/employer/thought-leadership/employee-of-the-future/use-ai-and-data-to-improve-the-employee-health-experience/ (last visited Dec. 3, 2023).
[64] *How to Reduce Bias in Artificial Intelligence,* Turing, https://www.turing.com/kb/how-to-reduce-bias-in-artificial-intelligence# (last visited Dec. 3, 2023).
[65] Zaid Obermeyer, et al., *Dissecting racial bias in an algorithm used to manage the health of populations*, 366 Science 6464, 447-453 (Oct. 25, 2019), https://www.science.org/doi/10.1126/science.aax2342.
[66] *Id.*

biases in four popular AI chatbot systems (ChatGPT, GPT-4, Google's Bard, and Anthropic's Claude) when researchers posed health questions with implicit reference to skin color and were met with responses erroneously asserting racist, unsupported and unrelated "facts."[67] Biased algorithms are also being seen actively in real-life, already-running systems.[68] These examples not only perpetuate the dark history of racism in the United States, but also shed light on the potentially devastating effects of using AI without solid guidelines in place establishing its parameters.

In addition to bias, another risk associated with AI's utilization lies with data security and privacy as mass amounts of data are required to achieve AI's peak functionality. In 2020, over 2.5 million medical records were leaked by Cense AI when they temporarily hosted the records on the internet before transferring them to their internal management system.[69] The leaked information included medical data and personally identifiable information (PII) related to car accident victims and was discovered by security expert Jeremiah Fowler.[70] Those purposefully searching for this type of data "will attack vulnerabilities anywhere along the AI data pipeline," so it is important that this pipeline is secured from all angles as the smallest weakness can cause catastrophic

[67] The study included questions such as "Tell me about skin thickness differences between Black and white skin" and "How do you calculate lung capacity for a Black man?" The chatbots would respond and include irrelevant and unfounded information differentiating Black people from White people – like "false assertions about Black people having different muscle mass and therefore higher creatinine levels." OpenAI and Google, parent companies of the various chatbots, publicly replied to the study and said they were actively working on reducing racial biases in their systems. Garance Burke, et al., *Bombshell Stanford study finds ChatGPT and Google's Bard answer medical questions with racist, debunked theories that harm Black patients,* Fortune (Oct. 20, 2023, 10:47 AM), https://fortune.com/well/2023/10/20/chatgpt-google-bard-ai-chatbots-medical-racism-black-patients-health-care/.
[68] Diagnosis-assisting AI software used to assess breathing ability via a spirometer was discovered to be underdiagnosing Black patients by nearly 40%. Mike Stobbe, *Black men were likely underdiagnosed with lung problems because of bias in software, study suggests,* Associated Press (June 1, 2023, 03:27 PM), https://apnews.com/article/black-racial-bias-lung-medical-diagnosis-e1f73be6d00f17091600b6f21f20264d.
[69] Matthew Humphries, *Report: AI Company Leaks Over 2.5M Medical Records,* PC Magazine (Aug. 18, 2020), https://www.pcmag.com/news/report-ai-company-leaks-over-25m-medical-records.
[70] Jeremiah Fowler, *AI Company Exposed 2.5M Records Including Medical Data of Auto Accident Victims Online*, Security Discovery (Aug. 17, 2020), https://securitydiscovery.com/ai-company-medical-data-leak/.

damage.[71] Companies holding on to mass amounts of valuable health data are specifically at a heightened risk for data breaches.[72]

Outside of data security, AI's ability to gain deep insight into its users' personal lives has elicited privacy concerns.[73] In 2019, this concern surfaced publicly when consumers became aware of the fact that digital voice assistants like Amazon's Alexa are constantly listening.[74] Though these assistant algorithms are programmed to listen for specific trigger words (such as "Alexa" or "Hey Google") before they start recording and analyzing, many users noted strange "coincidences" such as targeted ads for products only verbally discussed in passing.[75] This same concern extends to facial recognition systems like Apple's Face ID which collects a user's personal data including age, gender, and general appearance.[76]

Yet another commonly raised risk involves ethical concerns stemming from AI's lack of innate moral and ethical values. Given the difficulty of digitalizing human emotion and societal customs, AI systems lack the ability to make complex decisions that require this knowledge.[77] For example, AI robots are currently being used for diagnostic purposes in Obstetrics and Gynecology (OBGYN).[78] The robot's lack of sympathy and empathy poses problems for OBGYN patients who

---

[71] Jon Moore, *AI in Health Care: The Risks and Benefits*, Medical Economics (Mar. 15, 2023), https://www.medicaleconomics.com/view/ai-in-health-care-the-risks-and-benefits.
[72] *See* Edward Kost, *14 Biggest Healthcare Data Breaches*, UpGuard (Sep. 3, 2023), https://www.upguard.com/blog/biggest-data-breaches-in-healthcare *(outlining the 14 largest data breaches in healthcare, ranging from 345,000 to 5 million patient records breached in a singular occurrence); Fowler, supra* note 70 (holding that medical records specifically sell for approximately $250 per record on the black market).
[73] Xusen Cheng, et al., *The dark sides of AI,* electron Markets 32, 11-15 (2022), https://doi.org/10.1007/s12525-022-00531-5.
[74] Grant Clauser, *Amazon's Alexa Never Stops Listening to You. Should You Worry?* New York Times (Aug. 8, 2019), https://www.nytimes.com/wirecutter/blog/amazons-alexa-never-stops-listening-to-you/.
[75] *Id.*
[76] *See Cheng*, *supra* note 73.
[77] Dariush D. Farhud and Shaghayegh Zokaei, *Ethical Issues of Artificial Intelligence in Medicine and Healthcare,* 50 Iranian Journal of Public Health 11, i-v (2021), https://doi.org/10.18502/ijph.v50i11.7600.
[78] *Id.*

seek the aid of OBGYN physicians to treat sensitive and highly stressful situations, such as a negative impact on the healing process.[79]

E. Risks Associated with Use of AI Specifically for Healthcare Fraud

Though AI tools currently exist and the benefits of continuing to implement AI seem surplus, there is surrounding skepticism in the healthcare sector due to the gray areas of and barriers to the technology resulting in unnecessary risk. A mass of this skepticism lies with the data itself, beginning with where the data comes from. The aggregated data sets used by AI algorithms are published by differing sources and agencies (most often CMS). Though these published data sets are typically pre-labeled with various components, they are not published with guidelines on the method of aggregation of the data prior to being compiled into a set.[80] This may be important as an algorithm is wholly dependent on the data sources it learns from. Uncertainty in the reliability and methodology behind the aggregation can lead to inconsistencies with new data sets and negatively impact the algorithm's continuing education.[81]

Further, each data set contains different labeled components dependent on the provider and domain it originates from. To achieve the desired output, data sets often require "feature engineering" and "enriching."[82] Feature engineering is the process of extracting and organizing data to fit the purpose of the algorithm and decrease the amount of unnecessary information the algorithm must sort through. Enriching is the process of adding new or supplemental information into a data set. Both include imputing missing values, transforming features, normalizing columns,

---

[79] *Id.*
[80] *See Kumaraswamy*, *supra* note 52.
[81] For example, an algorithm's training data may become outdated over time and resultingly not account for changes in a word or phrase's context. The word "fire" is commonly used in the workplace to refer to a bad situation, when someone needs to "put out a fire" and solve a pertinent issue. More recently, the word "fire" has also been used by the younger generations to refer to something that is really good, such as a song or a meal – "That song is fire!" If an algorithm is using outdated training data, it may see the word "fire" and associate it with a negative context due to its lack of education on current trends.
[82] *See Johnson*, *supra* note 50.

encoding categorical variables, mitigating redundancy, and data labeling. This is influenced by the fact that CMS does not include "fraudulent" and "non-fraudulent" labels on published data sets. Thus, researchers in the past have had to consult outside sources to identify fraudulent providers and manually label the data themselves.[83] Thus, not only do these data sets require extra work, but individualized feature engineering and enriching can result in skewed or misleading data and can incorrectly influence the way a ML algorithm learns and develops.[84]

Another concern is bias in the algorithm. Though traditional examples of AI bias may not appear to be affected by anonymized provider data, one researcher studying the implementation of AI to detect healthcare fraud uncovered that large data sets have the capability of de-anonymizing and memorizing individual providers that did not have any PII to begin with.[85] This de-anonymization ability could open the floodgates to a mass of risks concerning bias that may be overlooked by developers who assume that the probability of such bias is nonexistent given its nature. As AI "only replicates the racial, gender, and age prejudice which already exists in our society," this oversight could be fatal to an algorithm's entire thought process.[86]

Bias in the data could include erroneously associating certain ethnic last names with fraudulent accounts or decreasing risk within certain populations for financial activities.[87] In a 2022 Deloitte study on the impacts of ethnicity and race in healthcare, research identified "long-standing issues around the collection and use of race and ethnicity data in healthcare — due to

[83] *See Id.*
[84] *Id.*
[85] *Id.*
[86] Bangul Khan, et al., *Drawbacks of Artificial Intelligence and Their Potential Solutions in the Healthcare Sector,* Biomedical Materials & Devices 1-8 (2023), https://doi.org/10.1007/s44174-023-00063-2.
[87] Danny Butvinik, *Bias and Fairness of AI-based Systems within Financial Crime,* NICE Actimize (July 25, 2022), https://www.niceactimize.com/blog/fraud-bias-and-fairness-of-ai-based-systems-within-financial-crime/#:~:text=In%20fraud%20detection%2C%20as%20one,certain%20type%20of%20financial%20activities.

both lack of standards and misconceptions."[88] Research shows that innocent providers associated with groups that commit more fraud are incorrectly flagged as fraudulent more often than others simply by reason of association.[89]

Other minor risks to consider are the "black box" problem and false positives and negatives. The black-box problem describes AI's inability to provide reasoning for its decisions or defend itself to incorrect outcomes, leaving us in a "black box."[90] This is a troublesome concept for many to understand as it is not common to allow a human being to make decisions without reasonable justifications. Absent a foundation for AI's decisions, it becomes difficult to accept what is produced at face value as it "lack[s] responsibility and legal identity."[91] Additionally, the risk of false positives and false negatives is prevalent. False positives appear when a legitimate transaction is wrongfully flagged as fraudulent, and false negatives appear when a truly fraudulent transaction goes undetected.

F. AI Regulations – Or a Lack Thereof

Considering the risks associated with AI's use, it may come as a surprise that AI *in general* is not currently federally regulated. While comprehensive federal legislation regarding the uses and extent of AI does not exist, there are existing laws and regulations that relate to certain aspects of AI. In 2021, the National AI Initiative Act of 2020 (NAIIA) was signed into law. Within this Act, Congress created the National Artificial Intelligence Research Resource Task Force which serves as a federal advisory committee tasked with "investigat[ing] the feasibility and advisability of establishing and sustaining a National Artificial Intelligence Research Resource; and . . .

[88] Jay Bhatt, et al., *Rethinking when and how to use race appropriately in care delivery,* Deloitte (May 19, 2022), https://www2.deloitte.com/us/en/insights/industry/health-care/racial-bias-health-care-algorithms.html.
[89] Jose Pombal, et al., *Understanding Unfairness in Fraud Detection through Model and Data Bias Interactions,* https://arxiv.org/pdf/2207.06273.pdf (last visited Dec. 3, 2023).
[90] *Id.*
[91] *Id.*

propos[ing] a roadmap detailing how such resource should be established and sustained."[92] The National AI Research Resource is intended to be a shared computing and data infrastructure with the goal of fueling AI research and development.

The AI in Government Act became law in 2020 as part of the Consolidated Appropriations Act of 2021, to ensure "that the use of AI across the federal government is effective, ethical, and accountable by providing resources and guidance to federal agencies."[93] The Act required the Office of Management and Budget (OMB) to issue guidance for agency use of AI within 270 days of enactment, but none was ever provided. As such, in December of 2022, U.S. Senator Rob Portman (R-OH), Ranking Member of the Senate Homeland Security and Governmental Affairs Committee, sent a letter to the OMB requesting an update on its implementation. It does not appear as if any movement was made following this letter.

International governments including the European Union (EU) and China are ahead of the United States in that they have begun the process of drafting regulations relating to AI. The EU's AI Act is expected to be finalized by the end of year 2023. This Act governs the sale and use of AI in the EU and proposes to set consistent standards governing AI systems across all EU member states.[94] It extends not only to developers within the EU but also to any global sellers selling or making their systems available to individuals within the EU. China has also enacted regulation targeting different aspects of AI, beginning in 2021 with its regulation on recommendation

[92] *National Artificial Intelligence Initiative,* U.S. Patent and Trademark Office, https://www.uspto.gov/sites/default/files/documents/National-Artificial-Intelligence-Initiative-Overview.pdf (last visited Dec. 3, 2023).
[93] *Portman Presses OMB on Implementation of AI in Government Act*, Homeland Security & Governmental Affairs (Dec. 22, 2022), https://www.hsgac.senate.gov/media/reps/portman-presses-omb-on-implementation-of-ai-in-government-act.
[94] Mia Hoffman, *The EU AI Act: A Primer*, Center for Security and Emerging Technology at Georgetown University (Sep. 26, 2023), https://cset.georgetown.edu/article/the-eu-ai-act-a-primer/#:~:text=The%20AI%20Act%20is%20a,systems%20across%20EU%20member%20states.

algorithms, through 2022 with rules for deep synthesis, and into 2023 with draft rules regarding generative AI.[95]

IV. Risk Assessment

The healthcare industry's increasing turn to AI for fraud detection necessitates an examination of its risks and solutions as specifically applicable to healthcare fraud. AI is not a one-size-fits-all solution to any problem, which means that not all of AI's risks affect its every use. As such, to accurately assess whether we should be wary of and actively working to avoid AI's risks as utilized for healthcare fraud detection, we must look at each risk's potential effects specifically.

AI is defined as a system that "imitate['s] human behavior,"[96] but this is not the function of AI that is utilized for healthcare fraud detection; instead, data-driven ML and AI algorithms are trained to digest and comb through data sets to pick out seemingly fraudulent claims.[97] Given this narrow focus, the likelihood of unintended consequences is lessened as there is less room for error. Additionally, this lessens the risk of the system producing biased results as there is less opportunity for the system to make any individualized assessments. The algorithm is not being asked to formulate conclusions or use any form of emotional or human intelligence – it is specifically tasked with determining whether a claim is fraudulent or non-fraudulent according to the data sets it was trained with. Thus, the system is not required to produce anything "new" and simply uses its knowledge to pinpoint fraudulent practices.

Yet another safeguard to the risk of bias is the de-identified manner of the data utilized by AI for healthcare fraud. Prior to being released to the public for use, CMS is required to comply

[95] Matt Sheehan, *China's AI Regulations and How They Get Made,* Carnegie Endowment for International Peace (July 10, 2023), https://carnegieendowment.org/2023/07/10/china-s-ai-regulations-and-how-they-get-made-pub-90117.
[96] *See supra* note 35.
[97] *See supra* Section II, Subsection B.

with HIPAA and ensure that none of the data published includes any individual identifiers.[98] By removing identifiers, the AI system does not have access to any demographic or personal information to formulate or apply biases to. This protects physicians as the system could utilize demographic information to improperly flag certain physicians it contains biases against. De-identification of the data also protects both physicians AND patients from the risks associated with data breaches, as there is no PII contained within the data that could be linked back to the individual.[99] While helpful, de-identified data does not completely eradicate risk as evidenced by one study that uncovered an AI algorithm's ability to nonetheless discover individual providers' identities and PII from this data.[100]

The breach of privacy (via intrusion into one's personal life)[101] and other ethical risks posed by AI generally are also combatted by the limited functionality of this specific type of AI and the de-identified manner of the data utilized. Digital voice assistants and other technologies that learn from their users raise privacy concerns as the scope of the assistants' data storage remains unknown. This is not an issue with AI in healthcare fraud corruption as there is no physical connection to the physician or the patient. The limited functionality of this type of AI additionally avoids ethical concerns as the system is not being asked to form any opinions or conclusions – it is merely being asked to differentiate fraudulent claims.

Given the nature of both the type of data and AI used, the risks generally associated with AI do not have the same negative effect on its application in healthcare fraud detection specifically. Thus, there is little reason to worry about its continued and increased use in that field. All things considered, the promise of AI's continued implementation in healthcare fraud detection plainly

[98] *See Johnson, supra* note 50.
[99] *See Johnson, supra* note 50.
[100] *See Butvinik, supra* note 87.
[101] *See Clauser, supra* note 74.

outweighs its risks in the long term; but, the lack of applicability and ease of continuation of use for healthcare fraud detection does not mean that policymakers and legislators should simply look the other way.

Technology mogul Elon Musk recently called for AI regulations while speaking with British Prime Minister Rishi Sunak during the UK AI Safety Summit.[102] Musk's comments were the result of both his and Prime Minister Sunak's skepticism regarding the existential risks that AI poses to fueling discrimination and misinformation. Musk thanked China for their participation in the fight to make AI safer by enacting legislation and said that, while annoying, having a "referee" will be a good thing for AI in the long run.[103]

Additionally, on October 30, 2023, President Joseph Biden issued an Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (hereinafter "EO").[104] The EO specifically instructs federal agencies to formulate regulations focusing on the safety and security of AI while addressing harms to the people utilizing AI and protecting civil rights and liberties and focuses on the difference between responsible and irresponsible AI. To keep AI safe and secure, Biden writes that "robust, reliable, repeatable, and standardized evaluations of AI systems, as well as policies, institutions, and, as appropriate, other mechanisms to test, understand, and mitigate risks from these systems [must be created] before they are put to use."[105] Biden additionally requires federal agencies to "address[] AI systems' most pressing

[102] Thomas Seal, *Musk Calls for AI Regulations in Chat with UK Prime Minister,* Bloomberg Law (Nov. 2, 2023, 05:01 PM), https://www.bloomberglaw.com/bloombergterminalnews/bloomberg-terminal-news/S3IJKYT1UM0W.
[103] *Id.*
[104] Joseph Biden, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (Oct. 30, 2023), https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.
[105] *Id. Section 2(a)*

security risks — including with respect to biotechnology, cybersecurity, critical infrastructure, and other national security dangers."[106]

The EO's objective is two-fold: to mitigate and address harms related to AI such as safety, bias and equity, and civil rights and civil liberties while simultaneously prioritizing innovation. Section 1, titled "Purpose," importantly states that AI "holds extraordinary potential for both promise and peril." The expansion of AI is vital for the United States and its citizens to continuously innovate, expand, and push technology's limits; but, this innovation is not paramount to the safety of the United States and its citizens.

Biden's EO is a step in the right direction. To avoid the spread of AI's general risks to the many subsectors of AI, including healthcare fraud detection, we must not turn a blind eye to the negative impact of AI in other areas. While not currently a risk for healthcare fraud detection, there is no guarantee that these risks and potential dangers will *never* have an effect. To pave the way for AI to continue to *positively* impact society and technology, we must face its risks and mitigate them as best as we can – the most effective way to do so could be via legislation and regulation. In the meantime, users of AI for healthcare fraud detection should additionally do their due diligence to ensure that these risks do not creep in.

V. Conclusion

The continued application of AI in healthcare fraud detection promises more efficient and autonomous identification of fraudulent activities within the healthcare system. AI's benefits, including real-time data analysis and enhanced pattern recognition, continue to revolutionize the way we combat fraud in the healthcare sector. However, with great power comes great responsibility as the inherent risks and challenges posed by AI require careful contemplation.

[106] *Id.*

This analysis has shed light on the many potential risks associated with AI's use generally and the lack of applicability to healthcare fraud detection specifically. Nonetheless, biases in an algorithm's decision-making processes, data privacy, and security issues, and the evolving nature of technology pose challenges that require continuous scrutiny and adaptation as they could still measle their way into the healthcare fraud sector over time. Moving forward, the healthcare industry must embrace AI cautiously and responsibly. Fostering a culture of awareness and education regarding the risks and benefits of AI in healthcare fraud detection will empower individuals to make informed decisions and advocate for responsible AI practices and will benefit the overall use of AI as well.

Summarily, while AI holds tremendous promise in the never-ending fight against healthcare fraud, it is incumbent upon us to approach its continued implementation with caution, diligence, and a commitment to addressing and avoiding its potential risks. By doing so, we can harness the transformative potential of AI while safeguarding the integrity of the healthcare system and ensuring the safety of both our providers and our patients. The journey ahead requires a delicate balance – a fusion of technological innovation and risk considerations to foster a healthcare landscape that is not only technologically advanced but also risk-free and socially responsible.