AI HEALTHCARE USE CASES
&
RISKS MANAGEMENT

AI WARRIORS ADVANCING YOUR BUSINESS TO NEW HEIGHTS

www.cahir.ai

Background:

Artificial intelligence (AI) has made significant advancement and impact across all major industries. Key advantages of integrating AI into business operations are broad and include automation of repetitive tasks, improved decision-making, enhanced customer experience, streamlined supply chain and logistics, risk management and fraud detection, cost savings and resource optimization, and increased innovation.

There are numerous benefits for implementing AI in healthcare ranging from enhanced diagnostic accuracy, faster turnaround time, personalized medicine, predictive analytics, clinical guidance, accelerated drug discovery, increased administrative efficiency, improved patient engagement, increased surgical accuracy, and better accessibility.

The possibilities with AI in the healthcare industry are limitless and with the rapid growth in AI, a talent gap has developed in the industry workforce. This is mainly caused by the rate of change of AI development and the need for an IT workforce. Putting money into an IT workforce within a company who understands the proper implementation of AI systems can take significant upfront time and financial investment. This typically causes many companies of different sizes and particularly smaller sized companies to be reliant on third parties and their expertise for the development of AI and cybersecurity systems within their industry.

Use Case Examples

The impact of AI in the healthcare industry has been disruptive and leaving profound many implications. The following are specific use cases and the type of AI which enables enhanced efficiencies, reduced costs and better patient outcomes. Use case examples include clinical decision support via improved diagnostics and personalized treatment plans, provider burnout and administrative work reduction via virtual assistants, and new drug discovery and formulation enhancement capabilities.

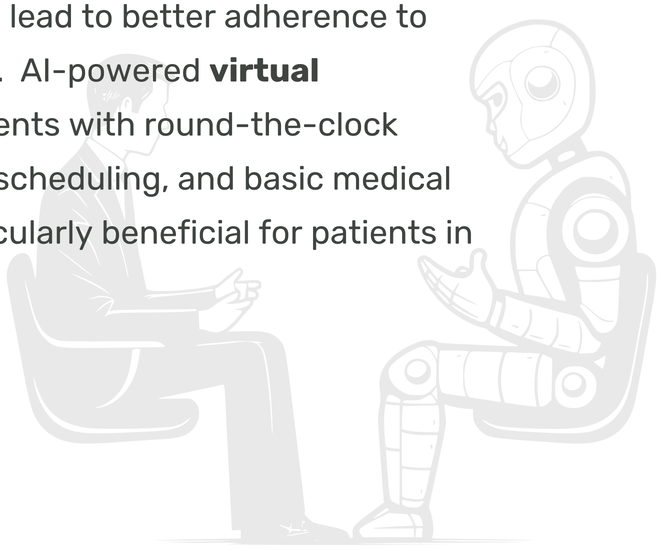
Predictive Analytics and Risk Assessment

AI can analyze patient data and environmental factors to predict disease outbreaks, enabling early interventions. AI can assess risk factors and predict potential health issues for individual patients. One of the most common uses of predictive analytics in healthcare is to identify patients at high risk of hospital readmission after discharge. Predictive models analyze factors like medical history, socioeconomic data, previous hospitalizations, and other variables to calculate a readmission risk score for each patient. This allows providers to implement targeted interventions like follow-up calls, home visits, or transitional care programs to reduce readmission rates.

On a broader scale, predictive analytics helps identify high-risk patient populations and potential disease outbreaks within communities. This enables proactive public health interventions and optimizes resource allocation for population health initiatives. Predictive analytics and risk assessment play a crucial role in healthcare by enabling early intervention, preventing adverse events, optimizing care delivery, and improving overall patient outcomes and population health management.

Improved Patient Engagement and Accessibility

AI-powered wearables, sensors, and telemedicine platforms enable remote patient monitoring and consultations, increasing healthcare accessibility. AI applications can provide personalized care recommendations and educational content, improving patient engagement. AI can analyze vast amounts of patient data to provide personalized insights, enabling healthcare providers to tailor their approach and communication to each patient's needs and preferences. This personalized engagement can lead to better adherence to treatment plans and improved health outcomes. AI-powered **virtual assistants** and **GTP chatbots** can provide patients with round-the-clock access to healthcare information, appointment scheduling, and basic medical advice. This increased accessibility can be particularly beneficial for patients in remote areas or with mobility issues.



Administrative Efficiency, Reduce Provider Burnouts and Cost Savings

AI can streamline administrative tasks like billing, appointment scheduling, and claims processing through automation, reducing costs and improving efficiency. AI can automate mundane and repetitive administrative tasks such as appointment scheduling, medical billing, data entry, and transcription of medical notes. This reduces the administrative burden on healthcare professionals, allowing them to focus more on patient care while minimizing errors and improving overall efficiency. **Natural Language Processing (NLP)** enables AI systems to accurately transcribe and interpret handwritten medical notes, clinical documentation, and other unstructured data sources. This streamlines the documentation process, reducing the time and costs associated with manual data entry. AI can automate the claims processing and billing procedures, reducing administrative costs associated with manual processing and minimizing errors that lead to claim denials and resubmissions.

Enhanced Diagnostic Accuracy

Deep learning AI algorithms can analyze vast amounts of medical data like images, test results, and patient records to accurately detect diseases and conditions at an early stage, reducing diagnostic errors. AI can identify patterns and abnormalities in medical images (X-rays, MRIs, CT scans) that may be missed by human experts, improving detection of cancers, fractures, and other conditions. For example, AI systems have shown impressive performance in detecting breast cancer from mammograms, with accuracy rates comparable to or exceeding those of experienced radiologists.AI can also assist in analyzing complex medical images like those from brain scans, helping diagnose conditions like Alzheimer's disease and stroke.

AI Lifecycle and Security Risks

The AI system lifecycle consists of three main phases: design, development, and deployment. Due to hasty design, development and implementation of AI systems across nearly all major industries, it became clear that security policies and procedures were needed for organizations to remain safe by managing AI risks and AI-enhanced cyberthreats.

National institutions like the National Institute of Standards and Technology (NIST), Cybersecurity Maturity Model Certification (CMMC), and International Organization for Standardization (ISO) developed and published industry best practices and standards. These standards were set in place to assist organizations in strengthening their defenses against risks introduced by AI and preparing organizations to embrace the new technology. NIST developed the Artificial Intelligence Risk Management Framework (NIST AI RMF) in response to calls for "operationalizing artificial intelligence ethics" and "translating principles into practice.. This framework explicitly directs organizations to consider the sociotechnical consequences of using AI for cybersecurity.

It's important to note that AI algorithms are intricately linked to their human creators and their lifecycle processes that designed and operationalized them. Humans possess unique capabilities, experiences, perspectives, and potential biases that could be introduced in any AI systems. Other considerations include data availability and quality itself used to train the AI which may have underlying noise, biased patterns, and other external issues. The inscrutability and lack of transparency to the AI development process itself often poses an additional risk factor.

AI Machine Learning Models and Adversarial Risks

A rising area of significant concern is adversarial AI. Adversarial AI and related tools deliberately and maliciously introduce factors and inputs that exploit AI systems' vulnerabilities. These adversarial related AI tools pose a significant challenge to businesses utilizing AIs across all industries. Adversarial tools are developed to hack and alter or disable the host's AI systems and baseline functions for malicious gains and criminal purposes. These are deliberate and malicious attempts in deceiving and manipulating AI machine learning models by exploiting underlying vulnerabilities. Some of the most common adversarial AI attack techniques include poisoning and transfer attacks.

The top 10 machine learning security risks are attacks in input manipulation, data poisoning, model inversion, membership inference, AI supply chain, transfer learning, output skewing, model theft, model skewing, and model poisoning.

In the healthcare industry, an adversarial input example involves creating and introducing fake data samples of medical imaging such as CT scans or X-rays that could cause an AI diagnostic system to misread or miss detect diseases, and ultimately leading to misdiagnosis.

In cybersecurity, examples include crafting adversarial network traffic data to evade cyber threat detection systems and bypass defenses to successfully enter networks. Adversarial malware could also have self-altering codes that bypass machine learning-based malware detection.

AI Risks Assessment and Management

Several frameworks and resources are available to guide organizations in developing their AI risk management strategies: NIST AI Risk Management Framework (AI RMF): This framework provides a structured approach to identifying and mitigating AI risks, emphasizing trustworthiness in AI systems. It includes a draft publication specifically addressing the risks associated with generative AI. Department of Energy's AI Risk Management Playbook: This playbook offers actionable pathways for AI risk identification and mitigation, focusing on responsible and trustworthy AI use. Other risk management frameworks for financial institutions include MITRE ATT&CK for Learning Systems (ATLAS), OWASP LLM Top 10 and Machine Learning Security Top 10.

These cybersecurity risk management strategies and practices include expanding existing cybersecurity systems and practices with new AI security technologies integration and increasing both cybersecurity information and fraud data sharing across vendors and institutions. A standardized and holistic trustworthy AI development framework and risk management protocols can effectively assess, monitor, protect, and prevent risks and adversarial attacks. Comprehensive AI risk assessment and management are critical for organizations navigating the complexities of AI technologies. By adopting structured frameworks, staying agile, and proactively addressing emerging risks, organizations can safeguard their operations and build trust among stakeholders. As the AI landscape continues to evolve, a robust risk management strategy will be essential for sustainable and responsible AI deployment.

Data Privacy

Ensuring data privacy in AI systems requires a comprehensive approach that spans the entire AI lifecycle, from data collection to deployment and operation. Key strategies include minimizing data collection, obtaining informed consent, and employing anonymization techniques.

Data Privacy Protocols

Data privacy protocols are also important in making sure quality healthcare data are being protected and shared safely. Organizations should establish standardized practices and guidelines to strengthen data use. Privacy by design should be integrated into AI development, emphasizing algorithmic integrity and data encryption. Robust access controls, continuous monitoring, and auditability are essential during deployment.

Organizations should conduct regular privacy impact assessments, adhere to data retention policies, and comply with regulations like GDPR. Training employees on privacy best practices and establishing ethical guidelines are crucial, as is evaluating third-party vendors for compliance. A tailored incident response plan should be in place to address any privacy breaches swiftly and transparently.

Lastly, fraud is increasingly cross-industry in nature. Sophisticated fraud rings and individuals often target multiple sectors rather than focusing on a single industry. Cross-sector collaboration in fraud prevention is becoming increasingly important, especially as fraudsters use sophisticated technologies like deepfakes and generative AI. Financial institutions, e-commerce sites, government agencies, and other sectors are realizing that sharing fraud data can drastically reduce crime and financial losses.

Resources

Risks Management Frameworks

- NIST AI Risk Management Framework (AI RMF)
- NIST AI RMF Playbook
- ISO/IEC 27001 and 27005
- OECD AI Principles
- EU AI Act
- MITRE ATT&CK for Learning Systems (ATLAS)
- OWASP LLM Top 10 and Machine Learning Security Top 10

Using Data In Healthcare

- Divatia, A. (2023, July 27). Adversarial Attacks On AI Systems. Forbes. https://www.forbes.com/sites/forbestechcouncil/2023/07/27/adversarial-attacks-on-ai-systems/
- Center for Open Data Enterprise. (n.d.). Sharing Health Data for Good. HealthDataSharing.org. https://healthdatasharing.org