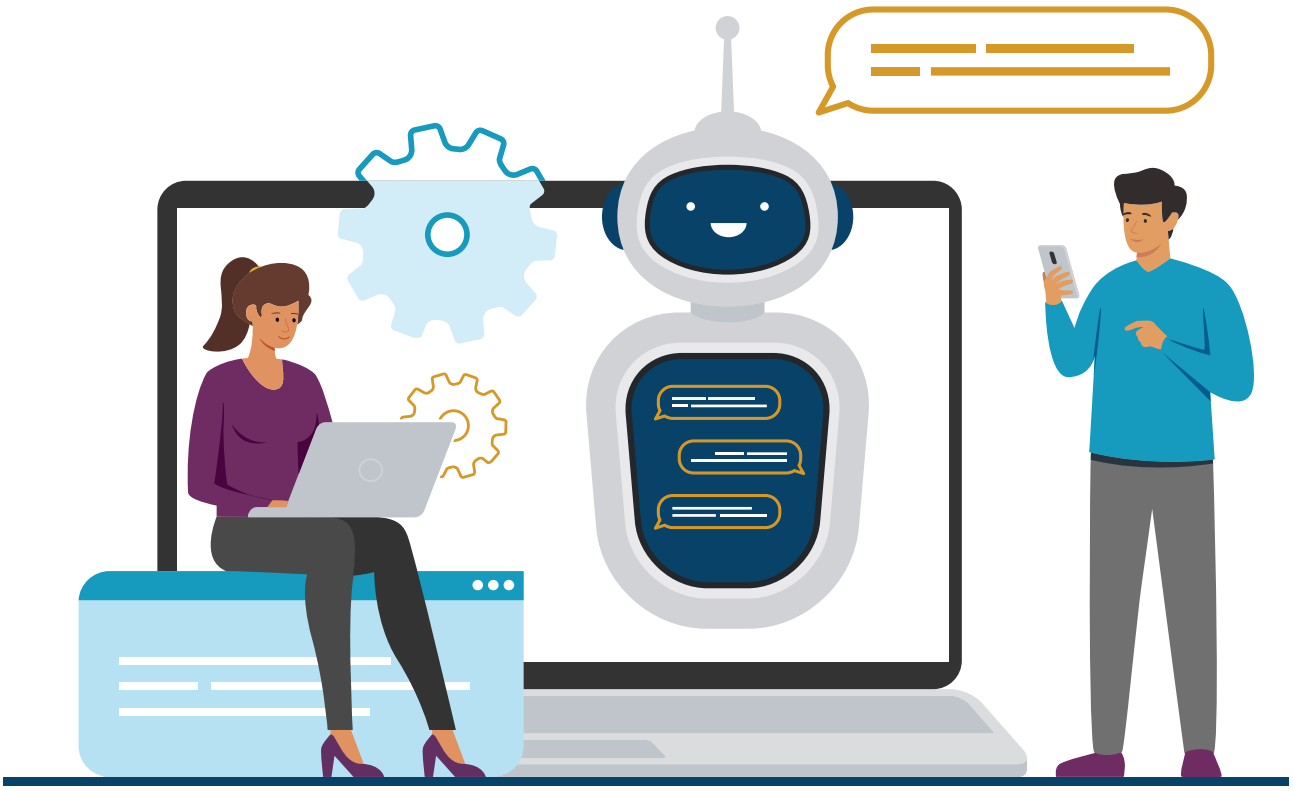
medisked

Artificial Intelligence in Health & Human Services



WHITE PAPER

Contents

Introduction

One of the business trends for 2023 has been the emergence of so-called **"Artificial Intelligence" (AI)** for the common man. (We use AI in quotes because there is not really a singular digital intelligence behind these programs in the way that we might think of the infamous Skynet from Terminator or VIKI from I, Robot).

Artificial intelligence as we know it through popular applications like ChatGPT, Google Bard, or Microsoft's Copilot, are written primarily in the form of **Large Language Models (LLMs)**. These tools are large collections of data, which their creators have fed into the system and are then processed through a series of complex rules (or algorithms) set forth by their developers.

The brilliance and allure of these tools is the simplicity of their use – no programming required. They make the information fed into their models available through **Natural Language Processing (NLP)**, which means you can type as if you were in a conversation with a human being and the LLM will provide more than just information matches (as does a search engine). LLMs will write a coherent response of the results in human-like text responses, from a simple answer to your question to writing the result in a usable business format, like a letter or memo in some cases. In fact, some parts of this white paper were written with the assistance of ChatGPT![1]

While these tools have been transforming many white-collar jobs, LLMs also have the potential to impact all of healthcare – not just the HCBS/LTSS industry – in various ways including clinical decision support, medical transcription and speech recognition, patient education, and telemedicine to name but a few. However, before turning over your clinical decisions to a digital LLM assistant, you would be wise to carefully contemplate the **privacy, security,** and **ethical** considerations involved in the deceptively straightforward response from your LLM of choice.

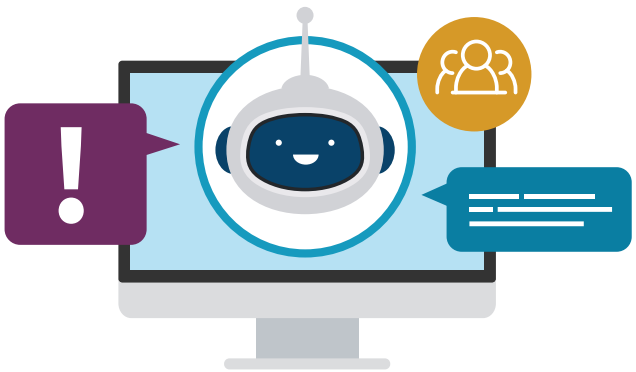
[1] https://openai.com/

Privacy Concerns

All healthcare providers have the responsibility to protect a patient's data hammered into them early in their careers. However, LLMs require a large amount of training data, which may include sensitive or private information. If the data used to train LLMs contains personal data, confidential business information, or other sensitive content, this raises concerns about data privacy and potential data breaches. There is usually little capability of the LLM to discern what is appropriate data unless trained by developers. Even then, users could enter sensitive information in a format the tool does not recognize and to a machine, data is just data. In fact, research indicates that **around 11% of data entered into ChatGPT by employees is sensitive information.**[2]

*Research indicates that **around 11% of data entered into ChatGPT by employees is sensitive information.**[2]*

Additionally, users may not have full control over the data they provide to LLMs and may not always be fully informed about how their data is used. This can raise concerns about consent, transparency, and control over personal information. Once an LLM has new data entered by a user, it becomes part of its data set and could be pulled out in another user's query. **Ultimately, the use of LLMs may raise concerns about compliance with data protection regulations, such as Health Insurance Portability and Accountability Act of 1996 (HIPAA)** or the General Data Protection Regulation (GDPR) in the European Union, as well as other applicable laws and regulations related to privacy, data security, and consumer protection. It is such a big concern that Italy recently took legal action to prevent ChatGPT from using its citizen's personal information in its training data.[3]



[2] https://www.darkreading.com/attacks-breaches/report-reveals-chatgpt-already-involved-in-data-leaks-phishing-scams-malware-infections
[3] https://www.wired.com/story/italy-ban-chatgpt-privacy-gdpr/

Security Concerns

Some information security concerns like **unauthorized access** to sensitive data, such as proprietary algorithms, training data, or other intellectual property is obvious at this point. However, this has become more than a theoretical threat. Just weeks after Korean tech giant Samsung lifted its ban on using ChatGPT, programmers entered sensitive code to get the tool to help troubleshoot it. Unfortunately, this made sensitive and proprietary code on semiconductors available to other unauthorized users.[4] Unauthorized access to LLMs, whether through data breaches or other means, can result in theft or misuse of this sensitive information, leading to potential intellectual property theft, competitive advantage loss, or other security breaches.

These tools can go far beyond troubleshooting code though; it can write code for you – even **malicious code** for threat actors. While ChatGPT has taken steps to reduce the tool's use for malevolent purposes, these filters are only in place for the free version. As a result, cybersecurity professionals are seeing a renaissance of creative, new malicious code and creative new phishing attacks developed by AI.[5]

Unfortunately, some of the sensitive corporate data that gets released to LLMs could be intentional. LLMs may be at risk of **insider threats**, where authorized users with access to the model misuse it for unauthorized purposes, such as generating fraudulent content, spreading misinformation, or abusing the model's capabilities. Insider threats can result in reputational damage, legal liabilities, or other security breaches.

LLMs can also be vulnerable to adversarial attacks, where inputs are intentionally crafted to manipulate the model's outputs. Firstly, LLMs may be susceptible to **model poisoning** attacks during the training process where an attacker injects malicious data into the training data to bias or manipulate the model's behavior. However, even once the model is trained, adversarial attacks can result in misleading or malicious outputs such as generating inappropriate or harmful content and can raise security concerns in applications such as content generation, automated writing, or chatbots. Ultimately these types of attacks can impact the integrity and reliability of the model's outputs, leading to potential misinformation, biased content, or compromised performance.

[4] https://www.theregister.com/2023/04/06/samsung_reportedly_leaked_its_own/

[5] https://www.darkreading.com/attacks-breaches/report-reveals-chatgpt-already-involved-in-data-leaks-phishing-scams-malware-infections

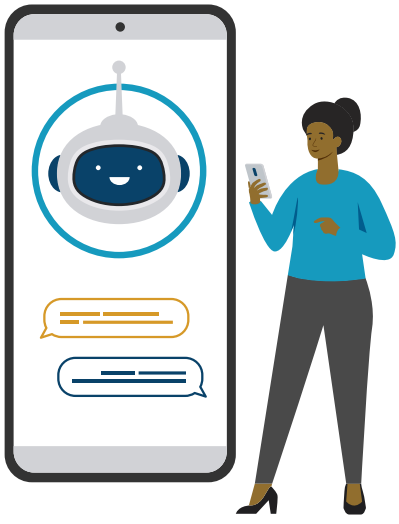
Artificial Intelligence and Human Services

Artificial intelligence will likely be as ubiquitous as the internet. All industries should be anticipating, evaluating, and actively shaping its trajectory. The US Department of Health and Human Services (HHS) has identified machine learning as a goal for person-centered outcomes by 2029 in their 2021 Report, *Building the Data Capacity for Patient-Centered Outcomes Research*, from the Office of the Assistant Secretary for Planning and Evaluation.[6]

At MediSked, we have been experimenting with natural language processing tools to extract and quantify written words and study subjective information. Data tools can examine unstructured data to analyze patterns and predict when a positive or negative event may occur. This data can help us identify opportunities for interventions and unmet needs sooner.

To find the true potential of AI in our space, every step must be thoughtfully made to ensure the protection of the individuals we support.

We have conducted NLP data studies to detect fluctuations in emotions or mental state over time and coordinate claims back to service note documentation for changes in health, housing, employment, circles of support, and other data. This can be used to improve outcomes and reduce costs by predicting and preventing negative consequences before they can occur. The purpose of our work is to help advance technologies for home and community-based services, but there is still much to be done. To find the true potential of AI in our space, every step must be thoughtfully made to ensure the protection of the individuals we support.



[6] https://aspe.hhs.gov/reports/building-data-capacity-pcortf-2021-annual-report

AI Study examining

The link Between Epilepsy Pharmaceuticals & Mental Health Side Effects

People with Epilepsy and their circles of support often notice higher rates of being depression, anxiety, and sometimes suicide. There is a difference between causation and correlation; many times it's not the Epilepsy, but instead it’s the medications for Epilepsy that cause these side effects. Certain drugs succeed in suppressing parts of the brain to avoid seizures but end up suppressing serotonin and other functions, leading to depression. Since 2008, the Food and Drug Administration (FDA) has required makers of Epilepsy drugs to include a warning about increased risk of suicidal thoughts and behaviors to those products’ prescribing information or labeling. While this may be true in some scenarios, it should not necessarily be applied to all drugs in this class.

We conducted a study with one of our developmental disability provider clients and a Developmental Disability Pharmacist to help identify signs of Epilepsy medication and depression using analytics. We examined data for individuals with a dual diagnosis of epilepsy and depression across a region in New York to identify the medications they are prescribed and the known side effects of these prescriptions. This allowed us to identify strategies and processes for medication review to lower impact of depression so people can live the highest quality life overlap of mental health, mental health and disability to be able to improve lives and outcomes of people with developmental disabilities. You can view a recording of the presentation here.

Conclusion

Despite the CEO of OpenAI saying the time of giant AI models is already over,[7] LLMs are probably here to stay. They are simply too helpful, convenient, easy to use, and for most purposes free… but they are also a great illustration of *caveat emptor* ("buyer beware"). If you choose to use these tools, you must keep in mind the significant privacy, security, and ethical concerns inherent to their use.

What is not in doubt is that at some level they will change the way we work. As individuals we must not let AI supplant our own common sense and intelligence in the way we do our jobs. As organizations, we need to be fully aware and educated about the potential risks from LLMs and assess the risk of using these technologies. Ultimately, as health and human service organizations, we must protect the people we serve – even from ourselves. We must not let the pursuit of efficiency blind us from our responsibility to improve lives.

The safest and most efficient way to utilize the benefits of artificial intelligence without putting the individuals you support at risk is to use a secure software solution with robust automation features. MediSked complies with the highest data security standards in the health and human services industry and our suite of solutions ensures that your staff can spend their time on what matters most – improving the lives of the individuals they support.

[7] https://aspe.hhs.gov/reports/building-data-capacity-pcortf-2021-annual-report

About the Authors

Shayne Champion is the Chief Information Security Officer (CISO) at MediSked, a CaseWorthy Company. With almost 30 years in Information Technology (IT) and Cyber Security industries, Shayne has experience spanning a wide range of technical domains. He has built, worked in, lead, and/or managed a wide variety of IT organizations prior to joining MediSked in 2020.

Linda Nakagawa is MediSked's Senior Industry Policy Analyst and has worked for MediSked, a CaseWorthy Company, for over six years. Before joining MediSked, Linda worked as a Policy Analyst at ADvancing States (formerly known as the National Association of States United for Aging and Disabilities).

MediSked is the leading brand in holistic solutions that improves lives, drives efficiencies, and generates innovations for health and human service organizations that support our community. MediSked solutions combine to provide innovative, person-centered technology that improves outcomes and quality, while reducing costs for individuals receiving home and community-based services and long-term services and supports through government & oversight, care coordination/payer and provider agencies. MediSked has supported clients across the United States since 2003.

Want to learn more? Check out medisked.com!