The Double-Edged Sword Of Using ChatGPT In Health Care

By **Aileen Murphy, Kara Du and Cynthia Suarez** (July 18, 2023)

Aileen Murphy

Kara Du

Cynthia Suarez

Since its launch in November 2022, OpenAI's ChatGPT has gained over a million users. ChatGPT is used by entities in a wide variety of industries.

On March 1, OpenAI updated its data usage policies[1] noting that (1) OpenAI will not use data submitted by customers to train or improve its models unless customers expressly opt-in to share such data, and (2) OpenAI will enter into business associate agreements in support of applicable customers' compliance with the Health Insurance Portability and Accountability Act.

With these changes, the growing publicity surrounding ChatGPT, and the expected growth of artificial intelligence in health care, entities and individuals in the industry will need to carefully consider and evaluate their use of ChatGPT to ensure their compliance with applicable privacy laws.

ChatGPT's Potential Uses in the Health Care Industry

It remains to be seen how exactly generative AI technology will reform the health care industry, but ChatGPT has already shown promising potential for use in several health care sectors:

Medical Education

Researchers from Massachusetts General Hospital and AnsibleHealth Inc. recently found that ChatGPT can almost pass the United States Medical Licensing Exam,[2] proving that ChatGPT may be a useful tool in the field of medical education, including as a study aide for future physicians and other health care providers by providing access to the works of some of the best health care clinicians in the world.

24/7 Medical Assistance

According to the Centers for Disease Control and Prevention, 6 in 10 adults in the U.S. have a chronic disease, such as heart disease, stroke, diabetes and Alzheimer's disease.[3]

Under the traditional office-based, in-person medical care system, access to after-hours doctors can be very limited and costly, at times creating obstacles to access such health care services. ChatGPT can potentially make a tremendous difference in this area, transforming in-person care to low-cost, around-the-clock AI-backed care.

For example, ChatGPT may help patients with chronic diseases by providing reminders of the need to schedule routine screenings, fill prescriptions, assist with other wellness matters such as monitoring steps taken, heart rates and sleep schedules, and customizing nutrition plans.

Routine Administrative Tasks

According to a 2018 cross-industry survey conducted by Spiceworks Inc., more than three-quarters of companies surveyed think AI will help automate routine tasks that take up unnecessary time and manpower, with up to 19% of these jobs potentially being handled by AI.[4]

For health care providers, ChatGPT can be trained to streamline patient intake processes, provide patients with answers to frequently asked questions, and compile patient records, which will help physicians to efficiently evaluate patient needs, provide diagnoses, and quickly identify treatment plans.

Medical Coding

ChatGPT can potentially be trained to comprehend Medicare and Medicaid codes, prepare billing reports and process claims, which would significantly reduce the workload for coders and also provide a potential backup confirmation to reduce potential billing and coding errors.

What Are the Potential Risks Involved?

While ChatGPT has the potential to be useful, the use of ChatGPT could also be a double-edged sword.

This may be particularly true in matters that pertain to data security and patient information privacy.

Despite its viral popularity, many organizations are wary about using ChatGPT. For example, JPMorgan Chase & Co. and Verizon Communications Inc. have restricted their employees from using ChatGPT, claiming they could lose ownership of customer information or source code that employees type into ChatGPT.[5]

The reason for such concern is that AI chatbots like ChatGPT rely heavily on the accuracy of vast quantities of online data.

In fact, as an open tool, the online data points that ChatGPT is trained on can be accessible to malicious actors who can launch attacks targeting this vulnerability. Alexander Hanff, member of the European Data Protection Board's support pool of experts, has warned "[i]f OpenAI obtained its training data through trawling the internet, it's unlawful."[6]

In the EU, for example, scraping data points from sites may potentially be in breach of the General Data Protection Regulation, the U.K. GDPR, the ePrivacy Directive, and the EU Charter of Fundamental Rights.[7]

Moreover, chatbots like ChatGPT that use automation functions, such as natural language processing and machine learning, could potentially result in serious consequences in the event of system failure if it is systematically adopted to engage in unstructured, open-ended dialogue with patients.

When a patient asks ChatGPT to answer some questions, provide information or perform tasks, the patient inadvertently hands over their protected health information and puts it in the public domain.

For instance, a patient that is concerned about being at risk of HIV exposure may enter his symptoms and ask the tool to check whether he is at risk. His symptoms, in addition to the conclusion generated, are now part of ChatGPT's database. This means the chatbot can now use this information to further train the tool and be included in responses to other users' prompts.

In addition to the foregoing, as the popularity and use of chatbots like ChatGPT evolves and grows, so does scrutiny from regulatory bodies.

Most recently, the Federal Trade Commission opened an investigation into OpenAI to determine whether the company has run afoul of consumer protection laws, including whether it has engaged in unfair or deceptive privacy or data security practices.[8]

In a civil subpoena issued to the company, which was made public on July 13, the FTC asked detailed questions about OpenAI's data security practices and its handling of users' personal information, including inquiries into what steps the company takes to prevent individuals' personal information from being included in the chatbot's training data and any mechanisms or processes in place to filter, anonymize or otherwise obscure such data.

Users of AI chatbots should be cognizant of potential scrutiny from state and federal regulators, and any resulting changes in regulation and oversight of these technologies.

What Safeguards Should Be Considered To Mitigate Risk?

As technology continues to develop, one of the key challenges for players in the health care space is balancing patient privacy and data protection with the benefits of utilizing technology.

The use of ChatGPT in the health care space could potentially require the collection and storage of vast amounts of PHI. However, HIPAA generally requires covered entities[9] to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose.[10]

So, for example, if a health care provider chooses to opt in to data sharing in order to train the ChatGPT model, they need to carefully assess how ChatGPT is being utilized, and whether any data entered could be considered PHI.

ChatGPT should be programmed, to the extent necessary to accomplish the intended purpose of its use, to only access and use PHI for specific, authorized purposes.

Health care providers that utilize ChatGPT should also implement strict security measures for storing and transmitting PHI and conduct regular risk assessments and audits to ensure compliance with HIPAA and any applicable state privacy laws.

Certain areas of focus include, but are not limited to:

Data Access

As mentioned above, ChatGPT's access to and use of PHI should be limited to specific, authorized purposes and covered entities should ensure proper training and protocols are in place for authorized personnel who access such PHI.

For example, under HIPAA PHI can be used and disclosed for billing of health care services.

If the intended purpose of using AI is to assist with billing, such purpose should be properly identified so that appropriate safeguards are in place to ensure that PHI is not being used by or disclosed to the AI technology for activities outside that scope.

Privacy Policies and Procedures

When implementing a new technology that potentially accesses or uses PHI, covered entities should update their HIPAA privacy and security policies to ensure there are safeguards and protocols in place to support the use of the new technology.

Business Associate Agreements

Prior to implementing any AI technology that processes, secures or accesses PHI, covered entities should enter into a business associate agreement with the vendor of such technology and ensure that appropriate provisions governing disclosure, use, and protection of such PHI, as well as notification and mitigation requirements in the event of a data breach or security incident, are in place.

Regular Security Training

Covered entities should keep employees up to date on security risks through regular security training.

Such training materials and programs should be updated to account for implementation of new technologies to ensure that potential risks particular to such technology are conveyed to workforce members and management teams.

Covered entities should also continually optimize security protocols — for example, implementing dual-factor authentication or anti-malware software to encrypt services.

Independent Verification

While ChatGPT and other AI technologies present potential benefits in making aspects of health care services delivery more efficient, such technologies cannot explain how they come up with their responses and therefore the decision-making processes cannot be verified.

Entities should consider the potential risks of biases in AI algorithms and variability in output and should independently verify the output of these technologies through regular testing and auditing.

Conclusion

Ultimately, ChatGPT and other AI technology may present opportunities for increased efficiency and greater quality of health care.

However, such opportunities must be carefully balanced against the risks related to patient data privacy, and covered entities should ensure that they have proper policies and procedures in place to mitigate these risks and appropriately track their use of ChatGPT or other AI technologies.

Aileen Murphy is special counsel, and Cynthia Suarez and Kara Du are associates, at Sheppard Mullin Richter & Hampton LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Data usage policies — OpenAI API.

[2] EXPERT REACTION: ChatGPT can (almost) pass the US Medical Licensing Exam — Scimex.

[3] Chronic Disease Center (NCCDPHP) | CDC.

[4] Spiceworks Study Reveals 40 Percent of Large Businesses Will Implement Intelligent Assistants or Chatbots by 2019 (prnewswire.com).

[5] JPMorgan Restricts Employees From Using ChatGPT — WSJ.

[6] #DataPrivacyWeek: ChatGPT's Data-Scraping Model Under Scrutiny From Privacy Experts — Infosecurity Magazine (infosecurity-magazine.com).

[7] ChatGPT vs GDPR — what AI chatbots mean for data privacy (information-age.com).

[8] FTC Civil Investigative Demand Schedule File No. 232-3044

[9] 45 CFR 160.103.

[10] Minimum Necessary Requirement | HHS.gov.