ChatGPT and Privacy Risks

Generative artificial intelligence technology chatbots rely heavily on the accuracy of vast quantities of online data **By Aileen Murphy, JD, Kara Du, JD, and Cynthia Suarez, JD**

SINCE ITS LAUNCH in November 2022, ChatGPT (GPT stands for Generative Pre-trained Transformer), a type of artificial intelligence model, has gained over a million users. ChatGPT is used by entities in a wide variety of industries. On March 1, 2023, OpenAI, the developer of ChatGPT, updated its data usage policies noting that (i) OpenAI will not use data submitted by customers to train or improve its models unless customers expressly opt-in to share such data, and (ii) OpenAI also will enter into business associate agreements in support of applicable customers' compliance with HIPAA.

With these changes, the growing publicity around ChatGPT, and expected increase in the use of AI in healthcare, entities and individuals in that space should carefully evaluate their use of ChatGPT to ensure compliance with applicable privacy laws.

Uses in the Healthcare Industry

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

- **Medical Education:** Researchers from Massachusetts General Hospital and AnsibleHealth found that ChatGPT can almost pass the U.S. Medical Licensing Exam, proving that ChatGPT may be useful in the field of medical education, including as a study aide for future physicians by providing access to the works of the best clinicians in the world.
- **24/7 Medical Assistance:** According to the CDC, 6 in 10 adults in the U.S. have a chronic disease, such as heart disease, stroke, diabetes and Alzheimer's disease. 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 healthcare 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 to schedule

routine screenings, fill prescriptions, and assist with other wellness matters such as monitoring steps taken, heart rates and sleep schedules.

- **Routine Administrative Tasks:** According to a new cross-industry survey conducted by Spiceworks, 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 percent of these jobs potentially being handled by AI. For healthcare providers, ChatGPT can be trained to streamline patient intake processes, answer patients' 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, significantly reducing the workload for coders and also providing a potential backup confirmation to reduce potential billing and coding errors.

What Are the Potential Risks?

While ChatGPT has the potential to be useful, it 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, organizations are wary about 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.

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 "If OpenAI obtained its training data through trawling the internet, it's unlawful." In the EU, for example, scraping data points from sites may potentially be in breach of the GDPR (and UK GDPR), the ePrivacy directive, and the EU Charter of Fundamental Rights.

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.

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 questions, provide information or perform tasks, the patient inadvertently hands over protected health information (PHI) and puts it in the public domain. For instance, a patient who 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.

Safeguards to Mitigate Risk

As technology continues to develop, one of the key challenges for players in the healthcare space is balancing patient privacy and data protection with the benefits of utilizing technology. The use of ChatGPT in the healthcare space could potentially require the collection and storage of vast amounts of PHI; however, HIPAA generally requires covered entities to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose. So, for example, if a healthcare 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.

Healthcare 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, 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 PHI.
- **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 new technology's use.
- **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 requirements in the event of a data breach, are in place.

Ultimately, the opportunities ChatGPT and AI technology may pose for increased efficiency and quality of healthcare must be carefully balanced against the risks to patient data privacy. Covered entities should have proper policies and procedures in place to mitigate these risks and appropriately track their use of ChatGPT or AI technologies.

The authors practice at Sheppard Mullin in its Corporate Practice Group; Aileen Murphy, JD, is special counsel in the firm's Chicago office; Kara Du, JD, is an associate; Cynthia Suarez, JD, is an associate in the firm's New York office.