FACT SHEET

GENERATIVE AI AND HEALTH DEPARTMENTS: LEGAL CONSIDERATIONS AND RISKS

INTRODUCTION

Artificial intelligence (AI), particularly generative AI, is being used with increasing frequency at all levels of federal and state government, including by state, tribal, local and territorial health (STLT) departments. Health departments are integrating it into multiple workstreams, including using it to prepare first drafts of documents, reports, and communication materials, using chatbots for customer service or healthcare queries, performing sophisticated data analysis, supporting food inspections, and many others. The Centers for Disease Control (CDC) has also expanded its AI use cases, which may pave the wave for STLT health departments to adopt additional uses as the track record for successful applications grow.

Amidst the growth of generative AI, there are also emerging legal risks and considerations that health departments will need to assess. Some of these considerations will affect all government agencies. Others, because of the type of work health departments do and sensitive data they may hold, may be more palpable for public health agencies as opposed to other types of government agencies or entities. This fact sheet highlights some topics of legal risk and considerations that health departments will want to review with their legal counsel.

OPEN RECORDS LAWS

All fifty states, the District of Columbia, and the federal government have laws requiring government records be made available to the public. These are sometimes referred to as public record laws or sunshine laws. While there is variation on public records laws from state to state, state to localities, and between states and the federal government, generally speaking most laws establish a definition of a record —with one notable exception being the federal Freedom of Information Act (FOIA), where agencies are encouraged to apply the definition of record in the Privacy Act— and the criteria around when it must be released. These laws often have built-in exemptions, such as for confidential data. In most instances, there is a presumption that records in an agency's possession are subject to release and the burden is on the agency to prove that an exemption applies.

Health departments should be aware that the use of generative AI, including prompts and chats, may create a record subject to public disclosure. Washington state has explicitly addressed this issue. In 2024, Washington's Secretary of State issued guidance on whether generative AI interactions are public records, stating that if "a generative AI interaction (input and output) relates to public business, then it is a public record"

The Network for Public Health Law

under state law. Furthermore, even if the state or local employee uses a personal AI account, if they are conducting business on behalf of the agency it is still a public record. The WA Secretary of State also issued guidance on how long generative AI records should be kept. Not all generative AI records need to be retained or kept for a uniform length of time; instead, it depends on the content and function of the record.

In addition, the City of San Jose has an AI policy which makes it clear that generative AI content, including prompts and outputs, may be subject to public records laws: "Any retained conversations relating to City work may be subject to public records requests and must comply with the City's retention policies. In addition, users will need to comply with the California Public Records Act and other applicable public records laws for all City usage of Generative AI. This means any prompts, outputs, or other information used in relation to a Generative AI tool may be released publicly. Unless you have been approved by the Information Technology Department (ITD) and are using a City enterprise Generative AI tool, do not use any prompts that may include information not suitable for public release."

Lastly, the state of Wisconsin's acceptable technology use, access, and security policy also discusses this issue. It states: "users should assume that any records and other electronic content on State-managed IT Resources (and content on personal devices) that are created or being kept in connection with the official purpose or function of the agency are 'records'" and includes generative AI output in the definition of records. Health departments will want to familiarize themselves with their state's open record law and any guidance that has been promulgated around how the law is interpreted with respect to generative AI inputs and outputs. Health departments should also be aware that information entered into generative AI is possibly a record that may one day be subject to a public record act request and retain records in accordance with the law.

PRIVACY AND SECURITY CONCERNS

The privacy and confidentiality concerns around generative AI are myriad and complex. First and foremost, not all commercially available large language models (LLM) like ChatGPT or Gemini are private. Inputting certain types of data into one of these open-source models may be a violation for a few reasons. The data has the potential to be impermissibly used or redisclosed in violation of the law. For example, a publicly available LLM, such as ChatGPT, may use data entered for training purposes. If HIPAA protected health information (PHI) is entered into the model without a patient authorization, and the model then uses the data for training, this is likely a HIPAA violation.

Furthermore, an entity that operates an LLM may be providing a business associate function or activity, if for instance, it is being used to provide data analysis for the HIPAA covered entity. If the company has not signed a business association agreement with the HIPAA covered entity however, this would also be a HIPAA violation. As such, agency staff should never enter confidential information into a publicly available LLM. Some agencies have procured generative AI models that are private and firewalled, often referred to as commercial LLM as opposed to a consumer LLM. With commercial models it may be permissible to input confidential data, but health departments will want to evaluate this with their IT departments and legal counsel.

Health departments that are HIPAA covered or HIPAA hybrid entities and are planning to use generative AI, will need to carefully evaluate how they will be using generative AI and with what type of data. If the health department's use implicates HIPAA protected data, such as a health chatbot that interfaces with patients of the department's primary care clinic, they will want to ensure they are complying with the HIPAA privacy and security rules, including how the information is used, disclosed, and secured while in transit and at rest. If the

health department is planning to use only de-identified data with generative AI or not input any data into a generative AI model, the exposure for any potential privacy issues are reduced.

COPYRIGHT CONSIDERATIONS

The copyright considerations around generative AI are extensive, with many being the subject of on-going litigation. Generative AI models are trained by ingesting large amounts of written material, some of which are copyrighted. The *New York Times* and other plaintiffs are suing OpenAI for copyright infringement, as are numerous other writers and artists. While these lawsuits are unlikely to directly affect health departments at this time, health departments should be aware of the potential for generative AI models to reproduce copyrighted works (among other content) nearly verbatim. While the likelihood of this remains low, it is not zero and in addition to the potential legal exposure, this could also erode public trust. In a case currently being litigated in the United Kingdom between Getty Images and Stability AI, Getty Images noted that some of the images produced by Stability's AI model even included the Getty watermark. Showing confidence in its own AI product, Microsoft announced in 2023 that it will defend customers and pay for any adverse judgments if they are sued for copyright infringement. In any event, health departments should remain vigilant about the potential for copyright infringement and ensure all work products are reviewed by a human.

Furthermore, the U.S. Copyright Office states that content generated solely by AI, or with "insufficient human control over the expressive elements" is not subject to copyright in the current regulatory environment. Health departments that wish to produce copyrighted materials should familiarize themselves with the current status of generative AI and copyright law and ensure the material meets the definition of copyrightable material.

CONCLUSION

The examples discussed above are far from an exhaustive list of the legal issues that can arise with generative AI. Additional areas for consideration include how to handle generative AI in litigation, AI procurement and vendor contracting, and others. And as new public health use cases of generative AI emerge, health departments will need to regularly evaluate AI usage and any corresponding legal risks and considerations.

This document was developed by Meghan Mead, J.D., Deputy Director- Mid-States Region. The Network promotes public health and health equity through non-partisan educational resources and technical assistance. These materials provided are provided solely for educational purposes and do not constitute legal advice. The Network's provision of these materials does not create an attorney-client relationship with you or any other person and is subject to the Network's Disclaimer.

SUPPORTER

Support for the Network provided by the Robert Wood Johnson Foundation. The views expressed in this document do not necessarily reflect the views of the Foundation.

Robert Wood Johnson Foundation