PATIENT PRIVACY IN THE AI ERA: Healthcare's New Data Dynamics

The influence of artificial intelligence (AI) on the medical field will be significant and rapid. With this breakthrough technology's swift advancement and adoption, lawmakers and courts must address a wide range of novel and challenging issues. Near the top of this list are questions surrounding the use of patient data.

Patient medical data is crucial for AI healthcare systems because it enables them to learn from diverse health records, improving their accuracy in diagnosing and treating patients. However, integrating this data into AI systems presents unique challenges and requires careful consideration of privacy laws. The recent case of *Dinerstein v. Google*, 73 F.4th 502 (7th Cir. 2023), highlights many of these associated complexities and provides a potential roadmap for other jurisdictions to follow.

As part of a research partnership, the University of Chicago Medical Center (UCMC) shared anonymized patient records with Google to facilitate the development of AI-driven predictive health models. A former UCMC patient sued both entities, alleging multiple legal violations. The U.S. District Court for the Northern District of Illinois dismissed the case, finding that the patient failed to state a claim and thus did not have standing to sue.

On appeal, the Seventh Circuit affirmed the dismissal, holding that the patient had not suffered a tangible injury due to the disclosure of his medical records. In reaching this conclusion, the court noted that most patient identifiers had been removed from the medical records, which sufficiently anonymized the data provided to the AI system.

In examining the possibility of future harm, the court acknowledged the theoretical possibility of identifying the patient by correlating his medical data with geolocation information but deemed such identification unlikely. In rejecting this potential "future re-identification" argument, the court noted that the alleged risk of future re-identification was not sufficiently imminent and could neither support monetary damages nor injunctive relief.

Dinerstein suggests that proper de-identification of medical records will be essential in reducing legal exposure when sharing patient data with AI systems. Conveniently, this approach aligns with the most well-known patient privacy law, the Health Insurance Portability and Accountability Act (HIPAA). Once data is de-identified according to HIPAA standards, it is no longer considered Protected Health Information and is not subject to HIPAA's use and disclosure restrictions.

While *Dinerstein* provides welcome guidance on this emerging issue, it remains to be seen if other jurisdictions will adopt a similar approach regarding patient privacy claims involving AI. Until then, providers utilizing AI systems should consider the following risk management steps to reduce legal risks when using patient medical data in AI systems:

1. Implement Robust Data De-identification
2. Ensure HIPAA Compliance
3. Obtain Patient Consent
4. Develop Clear Policies
5. Perform Regular Audits and Assessments
6. Stay Informed about Legal Developments

Disclaimer: If you would like to see the full sources for this article, go to ***https://bit.ly/3TAgxvy****.*

To explore more Risk Management resources, you can go to **RiskManagement.ProAssurance.com**. Or, use the helpline at **844-223-9648** or email **RiskAdvisors@ProAssurance.com**.

ProAssurance®