

10 Privacy Recommendations for Health App Developers From the AMA's Latest Privacy Principles

May 13, 2020

There has been no lack of new guidance regarding health care cybersecurity in recent weeks. But the American Medical Association's (AMA) newly released "[Privacy Principles](#)" is unique in its aim at entities involved in health care, but not otherwise covered by HIPAA. Increasingly, entities like health app developers gain access to valuable health care information free from HIPAA's reach. The AMA's new guidance makes clear, however, that these entities, at least in the AMA's view, are still responsible for safeguarding consumer privacy. The guidance includes in that responsibility the need to protect information that would historically not be considered personally identifiable, including IP addresses and advertising identifiers from mobile phones. And while the guidance is not binding, it will surely shape the applicable standard of care in future privacy litigation.

Here are 10 significant points for health app developers from the AMA's Privacy Principles:

1. At or before the time of collection, make sure consumers know what information you are accessing, using, disclosing, and processing. Don't use vague statements in a privacy policy that do not give consumers a meaningful understanding of what is happening.
2. Give consumers the right to control access, use, processing, and disclosure of their data on a granular, rather than document, level.
3. Give consumers the right to delete their information (exceptions apply).
4. Allow consumers the ability to access and extract their data in a machine-readable format.
5. Get opt-in consent before using a consumer's information to train machines or algorithms.
6. Minimize the collection and disclosure of health information.

7. Provide consumers who use apps to access their medical records the ability to annotate their medical records, and have mechanisms to record who made the annotation, how, when, and why.
8. Do not facilitate discrimination by, for example, creating and sharing risk scores or otherwise providing unconsented access to identifiable medical information that could form the basis for adverse decision-making.
9. Maintain the confidentiality of consumers' information.
10. Make your de-identification processes and techniques publicly available.

Authored By



Patricia M. Carreiro

Related Practices

[Health Care](#)

[Cybersecurity and Privacy](#)

Related Industries

[Health Care](#)

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.