PUBLICATION

Maryland's New Online Data Privacy Act: Sweeping Protections for Consumer Health Data and Implications for Health Care, Life Sciences, and AI

Authors: Alexandra P. Moylan, Michael J. Halaiko, Dandridge S. Parks
October 23, 2025

The Maryland Online Data Privacy Act (MODPA) became effective on October 1, 2025, and applies broadly to organizations handling Maryland residents' data, including many in the health care and life science industries. Although MODPA includes a certain familiar set of exemptions, it does not exempt nonprofits or HIPAA-regulated entities from its requirements. This narrow approach to exemptions, combined with new and stringent rules for health data, means health care, life science, health IT, and digital health organizations need to prepare now. See here for our previously released industry-agnostic alert discussing MODPA's general requirements.

What is Consumer Health Data?

MODPA intentionally extends the definition of Consumer Health Data beyond PHI or medical records to any data that is used by a controller "to identify a consumer's physical or mental health status." Consumer Health Data specifically includes data related to gender-affirming treatment and reproductive/sexual care. Other similar laws define the term Consumer Health Data much more narrowly. For example, the Connecticut Data Privacy Act defines it to mean only "personal data that a controller uses to identify a consumer's physical or mental health *condition or diagnosis*." Tying the definition to consumers' physical or mental health *status* means that data from over-the-counter purchases, mental and physical wellness apps, use of wellness products, and even general fitness information is Consumer Health Data if used to draw inferences about "health status."

The "Strictly Necessary" Data Minimization Standard

Consumer Health Data is classified as Sensitive Data under MODPA, which means it is subject to even more restrictions than other Personal Data regulated by the law. In addition to Consumer Health Data, Sensitive Data includes genetic and biometric information[1], precise geolocation, data about children, and data revealing race, ethnicity, religion, sexual orientation, sex life, transgender or nonbinary status, immigration status, and other protected characteristics.

For all categories of Sensitive Data, MODPA prohibits processing unless it is **"strictly necessary"** to provide the consumer with a *requested, specific product or service*. That standard applies regardless of consumer consent, which differentiates MODPA from other state privacy laws – other laws implement a "reasonably necessary and proportionate" standard and permit collection and processing with consumer consent. While MODPA includes a "reasonably necessary" standard, that standard applies to the collection and processing of consumer data that does not constitute Sensitive Data.

MODPA's "strictly necessary" standard for Sensitive Data is presumably a higher standard than "reasonably necessary," but MODPA does not define "strictly necessary." Accordingly, organizations will need to carefully consider whether their collection of Consumer Health Data, or other types of Sensitive Data, is strictly necessary. The law also permits processing of Personal Data, including Sensitive Data, for certain back-end or operational purposes. Controllers are permitted to process data for purposes beyond direct product or service delivery if the processing for (i) fraud prevention and detection, (ii) investigating and responding to security incidents, or (iii) internal operations reasonably anticipated by consumers, among others. Of these, the third

category could encompass a broad number of business activities. Enforcement actions may provide further insight into what the Maryland Attorney General deems "strictly necessary" when it comes to Sensitive Data and what operational activities satisfy the "reasonably anticipated by consumers" requirement for internal operations.

Other health-related restrictions include:

- **Geofencing prohibition**. The use of geofencing within 1,750 feet of a mental health facility or reproductive health facility for purposes of collecting or targeting Consumer Health Data is prohibited.

- **Absolute prohibition on the sale of Sensitive Data.** MODPA forbids the sale of Sensitive Data, regardless of consent. "Sale" is broadly defined to include exchange of personal data for "monetary or other valuable consideration." Organizations should scrutinize data-sharing arrangements to ensure compliance.

- **Mandatory Data Protection Assessments.** Collecting and processing Sensitive Data, including Consumer Health Data, requires controllers to conduct and document a Data Protection Assessment. The requirement explicitly extends to the use of algorithms analyzing Sensitive Data, potentially implicating machine learning and AI tools.

The law also requires organizations to strictly regulate access to Consumer Health Data. Employees and contractors must be subject to enforceable confidentiality obligations before gaining access to Consumer Health Data. Processors must satisfy MODPA's contractual and compliance requirements related to Data Processing Agreements in order to access and process Consumer Health Data on behalf of a Controller. These provisions will require organizations to update internal policies, vendor contracts, and other related agreements, to ensure compliance.

Relevant Exemptions for Health Care and Life Science Organizations

Like most similar laws, there are both data and entity-level exemptions built into MODPA. Notably, however, MODPA does not have an entity-level exemption for HIPAA-regulated entities or nonprofits.

Health-related data exemptions under MODPA include the following:

- PHI governed by HIPAA;

- Part 2 regulated substance use disorder records (42 U.S.C. § 290dd–2);

- Federal human subjects research data collected and used for research regulated by the Common Rule (45 C.F.R. § 46);

- Human subjects research data collected and used in compliance with the International Council for Harmonization (ICH) Good Clinical Practice (GCP) guidelines;

- Data collected and used for public health, community health, or population health activities and purposes, as authorized by HIPAA, when provided by or to a HIPAA regulated entity;

- Patient Safety Work Product created under the federal Patient Safety and Quality Improvement Act;

- Medical records subject to the Maryland Confidentiality of Medical Records Act (MCMRA), where held by a covered entity or business associate that applies HIPAA/MCMRA standards for collection, use,

and disclosure; and

- Information de-identified in accordance with HIPAA.

Health care and related organizations should carefully map which data sets fall within these carveouts and which do not. Data outside of these categories, potentially including wellness data, mobile app information, consumer-generated health information, or research not covered by the Common Rule or ICH guidelines, remains within scope.

What is De-identified Data?

MODPA adopts the definition of De-identified Data set forth in Maryland's Genetic Information Privacy Act (Md. Code Ann., Commercial Code, § 14-4401), which is data that (1) cannot reasonably be (i) used to infer information about a consumer, or (ii) linked to an identifiable consumer and (2) that is subject to (i) administrative and technical measures to ensure that the data cannot be associated with a particular consumer; (ii) public commitment by the company to maintain and use data in a de-identifiable form and not attempt to reidentify data, and (iii) legally enforceable contractual obligations that prohibit a recipient of the data from attempting to reidentify the data.

De-identified Data is largely exempt from MODPA's requirements, provided that controllers who disclose such data:

1. Exercise reasonable oversight to monitor compliance with any contractual restrictions imposed on the recipient; and

2. Take appropriate steps to address any violations of those commitments.

This obligation is ongoing; de-identification is not a one-time safe harbor. Organizations must maintain contractual and technical safeguards and exercise continuous oversight of downstream use. For de-identification of Sensitive Data, controllers should consider implementing more stringent contractual protections and audit rights because the law specifically contemplates a higher standard of oversight when it comes to De-Identified Data that would be Sensitive Data if reidentified.

Notably absent from the law are definitions or exemptions for anonymized or pseudonymized data. This creates regulatory uncertainty, making it challenging for organizations to determine the appropriate safeguards and compliance measures for data that falls short of full de-identification but is not directly identifiable.

Implications of MODPA for AI in Health Care

MODPA's enhanced restrictions on collecting and processing Sensitive Data will have a significant impact on the development and use of AI systems in health care and related sectors. Organizations should promptly identify and document all AI use cases that involve Sensitive Data, including Consumer Health Data, to ensure compliance with MODPA. Key steps include mapping data flows, updating internal policies and procedures, and implementing technical safeguards to meet legal requirements. MODPA may restrict the use of Consumer Health Data or other Sensitive Data for AI model development, requiring organizations to reevaluate their AI strategies, data governance, and risk management practices.

Practical Next Steps and Takeaways

Because of its broad definitions and novel restrictions, it will be important to continually monitor MODPA and how strictly the Attorney General interprets it. The following high-level steps are a good starting point for MODPA compliance:

- **Scope Analysis**: Confirm whether your organization meets MODPA's volume/revenue thresholds.
- **Map and inventory data:** Identify all data tied to Maryland residents, focusing on non-PHI health information, Consumer Health Data, and Sensitive Data.
- **Reassess Sensitive Data collection:** Ensure collection of genetic, biometric, or other Sensitive Data can be justified as "strictly necessary."
- **Update contracts and policies:** Incorporate confidentiality obligations into workforce agreements and update vendor contracts to address Consumer Health Data.
- **Revisit deidentification:** Confirm deidentification aligns with MODPA's requirements.
- **Review research data practices:** Confirm whether human subjects research data qualifies for a carveout and determine if other research datasets fall outside of MODPA.
- **Plan for Data Protection Assessments:** Develop processes for documenting assessments, especially for AI tools and research programs involving Sensitive Data.
- **Evaluate AI usage:** Document all administrative and clinical AI systems that may involve Sensitive Data.

MODPA will be enforced by the Maryland Attorney General, with violations treated as unfair or deceptive trade practices. While a limited cure period applies through April 2027, health care, health IT, and life sciences organizations should act now. Mapping non-PHI data, reassessing deidentification protocols, revising contracts, and developing assessment processes will be essential steps toward compliance. For assistance in assessing your organization's strategic data goals and compliance readiness under MODPA or other U.S. state privacy laws, please contact Alexandra P. Moylan, Michael J. Halaiko, Dan S. Parks or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.

---

[1] MODPA's definition of biometric data is broader than that found in other state laws. Whereas other state laws define biometric data to be data generated by automatic measurements of the biological characteristics of a consumer used to uniquely authenticate a consumer, MODPA broadens the definition to mean data that **can be** used to uniquely identify a consumer.