BCLP. Client Intelligent

Insights

EXPANSION OF CONNECTICUT DATA PRIVACY ACT

Jun 30, 2023

As with a growing number of states, Connecticut passed a comprehensive consumer privacy law, the Connecticut Data Privacy Act (the "CTDPA"), on May 10, 2022. The CTDPA became effective on July 1, 2023 and, in spite of that effective date, was revised in early June by the Connecticut legislature to include some notable protections for health data and minors. The updated version, Public Act No. 23-56 (formerly SB 3), was signed by the governor on June 26, 2023, and set the effective date for the health data amendments at July 1, 2023, giving companies basically no time to comply. There is, however, additional time to comply with certain obligations covering minors (either July or October of *2024*).

These amendments are consistent with the increased interest – at the federal and state level – in protecting health data not already covered by the federal Health Insurance Portability and Accountability Act or HIPAA. Indeed, the Connecticut Attorney General, who has exclusive enforcement authority under this law, recently released a short guidance document on the Act, suggesting the AG will be taking compliance and enforcement seriously.

As noted, Connecticut is not alone in its focus on health data. The state of Washington recently passed the My Health My Data Act (the "MHMDA"), and Nevada passed a similar law. See our blog post for more information on the MHMDA.

CONSUMER HEALTH DATA

The CTDPA health data amendments are likely narrower than the provisions of the MHMDA, but the revisions are still notable and require attention by organizations subject to the law. Below we address some of the key revisions.

Although the CTDPA already includes "data revealing…mental or physical health condition or diagnosis" within the definition of "sensitive data," the amendments introduce a new definition of "consumer health data" and tie additional obligations to organizations that collect and use such information. "Consumer health data" is defined as "any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data."

The new rules that apply to consumer health data include:

- **Consent**: As with all categories of sensitive data, organizations must obtain affirmative opt-in consent before processing consumer health data.
- **Employee restrictions**: Section 2 of the law, which is new, requires that employees or contractors with access to consumer health data be subject to contractual or statutory duties of confidentiality.
- **Geofencing restrictions**: The law now prohibits the use of geofences (any technology that uses certain location data, like GPS coordinates or cellular data, to establish a virtual boundary) within 1,750 feet of any mental, reproductive, or sexual health facility for the purpose of, for example, collecting consumer health data or sending notifications to a consumer regarding their consumer health data.
- **Sale of consumer health data**: Sales of consumer health data – as in, exchanges of consumer health data for money or other valuable consideration – are not allowed under the amendments without consumer consent.

As noted above, these new obligations became effective on July 1, 2023, with the rest of the CTDPA, but from July 1, 2023 to December 1, 2024, the AG *must* issue a notice of violation to a controller if cure of the violation is possible, and the controller has 60 days to cure the violation. Starting January 1, 2025, the cure period will be granted at the AG's discretion.

PROTECTIONS FOR MINORS

The CTDPA amendments that apply to data of minors – i.e., consumers under 18 – include the following:

- **Unpublish requests**: Section 7 requires social media platforms, upon request, to "unpublish" a minor's social media account within 15 days. In other words, the account has to be removed from "public visibility."
- **Deletion requests**: If a platform receives a separate deletion request, it has 45 days to delete the account and stop processing the minor's data, which includes the collection, storage, or use of the data.
- **Reasonable care to avoid harm**: Controllers must "use reasonable care to avoid any heightened risk of harm to minors caused by" the online product or service. A "heightened risk of harm to minors" includes, among other things, processing a minor's "personal data in a manner that present[s] any reasonably foreseeable risk of" unfair or deceptive treatment.

- **Restrictions on processing**: Absent the appropriate consent (affirmative opt-in), a controller cannot process a minor's personal data for the purposes of targeted advertising, the sale of personal data, or profiling, unless the processing is necessary to provide the relevant service. Without consent, controllers are also prohibited from collecting a minor's precise geolocation unless the data is reasonably necessary for the service *and* the controller signals to the user that geolocation is being collected.
- **Data protection assessments**: Controllers must conduct certain data protection assessments for their online service. The assessments must address the purpose of the online service, the categories of a minor's personal data processed, the purpose of the processing, and any heightened risk of harm to the minors.
- **Exemptions**: Like the new provisions governing consumer health data, this section has a long list of similar exemptions, as well as certain carve outs for compliance with the Children's Online Privacy Protection Act or COPPA.

These provisions discussed above come into force either on July 1, 2024 (unpublish and deletion requests) or on October 1, 2024, with a similar mandatory cure period that lasts until January 1, 2026.

WHAT SHOULD YOUR ORGANIZATION DO TO PREPARE?

In spite of the effective date of the health data amendments, the good news is that unlike the Washington My Health My Data Act, the CTDPA does not contain a private right of action. Nevertheless, organizations should not underestimate the impact of potential enforcement action as well as the time needed to comply with these new and complicated rules. Therefore, companies should work to:

- Understand the potential in-scope data (particularly health and minor data), as well as the underlying purposes of use, sources, and potential recipients;
- Analyze and document whether any exceptions apply (e.g., HIPAA, COPPA);
- Evaluate where current disclosures, consent mechanisms or other compliance efforts may already address certain requirements of the law and/or can be updated for these purposes;
- Begin building required additional notices and consents and authorizations; and
- Stay tuned for additional guidance from the BCLP Global Privacy and Security team.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Goli Mahdavi

San Francisco

goli.mahdavi@bclplaw.com
+1 415 675 3448