Minnesota Consumer Data Privacy Act

Michael Cohen

May 23, 2025

Lathrop GPM

What We Will Cover Today

- Overview of Minnesota Consumer Data Privacy Act
- Exemptions Relevant to Ambulatory Surgery Centers
- Potential Actions to Comply and Mitigate Risk

A Legal Guide To PRIVACY AND DATA SECURITY

2025

A Collaborative Effort

Minnesota Department of Employment and Economic Development

Lathrop GPM

New and Emerging State Data Privacy Laws

- In 2018 California became the first state to enact a comprehensive data privacy law ,the California Consumer Privacy Act (CCPA) followed by the California Privacy Rights Act (CPRA) in 2020
- Minnesota has joined 18 other states – California, Virginia, Delaware, Connecticut, Colorado, Iowa, Maryland, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Indiana, Kentucky, Rhode Island, and Utah – that either have comprehensive data privacy laws in place or have laws that take effect in 2025.

Minnesota Consumer Data Privacy Act (“MCDPA’)

- For overview of MCDPA see my client alert prepared when law passed last year- https://www.lathropgpm.com/insights/minnesota-enacts-comprehensive-data-privacy-law/

Overview of MCDPA

- The MCDPA takes effect July 31, 2025, and covers legal entities that conduct business in Minnesota or produce products or services targeted to state residents and that satisfy one or more of the following:

(1) during a calendar year, control or process the personal data of at least 100,000 consumers (excluding payment transactions); or

(2) derive over 25% of gross revenue from the sale of personal data and processes or controls the personal data of at least 25,000 consumers.

- Does your ASC fall within 100,000 threshold?
- In health care context, “consumers” likely means “patients” and “processes” likely includes storing patient information

MCDPA and HIPAA

- The MCDPA applies to a broader range of personal data, while HIPAA specifically covers protected health information (PHI).
- Covered entities and business associates under HIPAA are exempt from the MCDPA to the extent they collect and process PHI.
- Is your ASC a “covered entity”?
  - Provider of medical or other health services or supplies
  - That transmits any health information in electronic form
  - In connection with HIPAA “covered transactions”

Refresher: What is PHI / Health Records?

- PHI (42 C.F.R. 160.103):
  - "***Individually identifiable health information***" (subset of health information, including demographic information collected from an individual, and: (1) Is ***created or received by a health care provider,*** health plan, employer, or health care clearinghouse; and (2) ***relates to the past, present, or future*** physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that ***identifies the individual***; or (ii) with respect to which there is a ***reasonable basis to believe*** the information can be used to identify the individual) that is transmitted by electronic media, maintained in electronic media, or transmitted in any other form or medium
- Health Records (Minn. Stat. 144.291):
  - Any information, whether oral or recorded in ***any form or medium***, that ***relates to the past, present, or future*** physical or mental health or condition of a patient; the provision of health care to a patient; or the past, present, or future payment for the provision of health care to a patient.

Consumer Defined

- The MCDPA defines "consumer" as a natural person who is a Minnesota resident acting only in an individual or household context. Consumer does not include a natural person acting in a commercial or employment context.
- This means that **the MCDPA does not apply to personal data relating to job applicants, employees, and individuals acting in their capacity as business representatives.**

Personal Data Defined in MCDPA

- Personal data is defined as “any information that is linked or reasonably linkable to an identified or identifiable natural person.”
- Personal data does not include deidentified data or publicly available information.
- “Publicly available information" means information that (1) is lawfully made available from federal, state, or local government records or widely distributed media, or (2) an organization has a reasonable basis to believe has lawfully been made available to the general public.

Enhanced Rights for Consumers Under MCDPA

- The MCDPA provides consumers with the right to:
- Confirm whether an organization is processing personal data about the consumer and to access the categories of personal data processed by the organization ;
- **Correct** inaccurate personal data concerning the consumer, taking into account the nature of the data and purposes of processing;
- **Delete** the consumer's personal data (subject to exceptions);
- Obtain a copy of personal data that the consumer previously provided to the organization, where the data processing is conducted by automated means; and
- Obtain a list of the specific third parties to whom the organization disclosed the consumer's personal data or, if not available, a list of the specific third parties to whom the organization has disclosed any consumers' personal data.

Responding to Data Subject Access Requests

- Must provide one or more secure means for submitting request
- Must respond and comply within 45 days of receipt of request
- May extend for additional 45 days if reasonably necessary
- Must notify of appeal process with instructions on how to file a complaint with Minnesota Attorney Generals Office
- Maintain records of all appeals for 2 years
- Not required to comply with request if unable to authenticate
- Must not disclose social security number, financial account number, drivers license, health insurance account, or medical identification number (only that you have collected that type of information)

Privacy Policy

- The organization must provide consumers with a privacy notice that includes **the categories of personal data** processed,
- **purposes** for which categories of personal data are processed,
- an **explanation of the consumer rights and how to exercise the rights** including **how to appeal** actions taken with regards to a consumer request
- **categories of personal data that organization sells or shares with third parties,**
- **categories of third parties**, if any, with whom organization sells or shares personal data,

Privacy Policy

- Contact information, including active email address that consumer may use to contact organization,
- Description of data retention policies,
- Date privacy notice was last updated,
- If personal data is sold to third parties or organization processes data for targeted advertising the organization **must disclose the processing in notice and provide method to opt out of sale or processing** which can be hyperlink labelled Your Opt-Out Rights or Your Privacy Rights

Profiling

- The law includes new consumer rights and obligations around profiling practices. **Consumers can request information regarding a profiling decision carried out against them,** including the reasoning behind a particular profiling decision and access to the data used to reach the decision.

Data Inventory Requirement

- The organization may need to maintain a data inventory and document its policies and procedures used for data security and to comply with the law.
- The MCDPA states that a “controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data, ***including the maintenance of an inventory of the data that must be managed to exercise these responsibilities*****.** The data security practices shall be appropriate to the volume and nature of the personal data at issue.”

Data Retention

- The MCDPA provides that a **“controller may not retain personal data that is no longer relevant and reasonably necessary in relation to the purposes for which the data were collected** and processed, unless retention of the data is otherwise required by law or permitted under a statutory exception such as performing a contract to which a consumer is a party, fulfilling the terms of a written warranty, and others specifically listed in the MCDPA.

Universal Opt-Out Mechanisms (“UOOM”)

- The MCDPA also includes requirements for recognition of universal opt-out mechanisms.
- This means that consumers can use a UOOM, like a browser extension or setting, to automatically tell the business or organization they do not want their personal data sold or used for targeting advertising and such requests must be honored.

Data Protection Assessments

- The MCDPA requires the organization to conduct "**data privacy and protection assessments" for certain processing activities, including processing personal data in connection with targeted advertising, sales of personal data, processing sensitive data,** profiling that presents a heightened risk of harm to consumers and profiling that presents certain types of foreseeable risks (e.g., unfair and deceptive treatment, financial or reputational injury, intrusion on seclusion, etc.).
- The organization **needs to document and retain such assessments and make them available to the Minnesota Attorney General upon request.**

Third Party and Service Provider Agreements

- Must have compliant agreement with any party that processes personal data on your behalf
- Duty of confidentiality
- Appropriate technical and organizational measures to ensure security
- Identify purpose of processing and restrict to designated purpose
- Other provisions as required by MCDPA
- Business Associate Agreement may suffice

Enforcement

- The MCDPA is **enforceable by the Attorney General's office**.
- There is **no private right of action.**
- Violations of the MCDPA are subject to injunctive relief and civil penalties up to $7,500 per violation.
- The Minnesota Attorney General is required to provide the organization with notice of the specific provisions of the MCDPA that it alleges have been violated and 30 days to cure the violations prior to bringing an enforcement action. **This cure provision expires on January 31, 2026.**

MCDPA Exemptions

- The MCDPA includes exemptions for certain types of businesses and data.
- Governmental entities, federally recognized Indian tribes, “small business” as defined by the U.S. Small Business Administration regulations, air carriers under the Airline Deregulation Act, and certain kinds of banks, credit unions and insurance companies are exempt.
- The MCDPA does not include an entity-level exemption for companies that are covered entities or business associates under HIPAA.
- The data-level exemptions are consistent with most other state privacy laws. **Specifically, the MCDPA exempts data regulated by HIPAA,** the Minnesota Health Records Act, Part 2 (substance use disorder information), the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Driver’s Privacy Protection Act, the Family Educational Rights and Privacy Act, the Farm Credit Act, the Minnesota Insurance Fair Information Reporting Act, and various other regulations.

Health and Medical Data Exemptions

- (i) protected health information, as defined by and for purposes of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and related regulations;
- (ii) health records, as defined in Minnesota Health Records Act [section 144.291], subdivision 2
- (iii) patient identifying information for substance abuse records established pursuant to United States Code, title 42, section 290dd-2;

Health and Medical Data Exemptions

- information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, Public Law 99-660, and related regulations;
- patient safety work product for purposes of Code of Federal Regulations, title 42, part 3, established pursuant to United States Code, title 42, sections 299b-21 to 299b-26;

HIPAA Covered Entity and Business Associate Exemption

- information that is derived from any of the health care-related information that has been deidentified in accordance with HIPAA;
- information originating from, and intermingled to be indistinguishable with, any of the health care-related information listed in MCDPA that is maintained by:

(i) a covered entity or business associate, as defined by the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and related regulations;

(ii) a health care provider, as defined in Minnesota Health Records Act section 144.291, subdivision 2; or

(iii) a program or a qualified service organization, as defined by 42 CFR part 2

HIPAA Covered Entities Exempt for PHI

- information that is:
- (i) maintained by an entity that meets the definition of health care provider under Code of Federal Regulations, title 45, section 160.103, to the extent that the entity maintains the information in the manner required of covered entities with respect to protected health information for purposes of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and related regulations
- Information that is included in a limited data set (as defined under HIPAA)

Potential Action Items

- Determine if your organization is covered by law
- To what extent do HIPAA, MHRA and related exemptions apply
  - What information would any ASC maintain that is NOT going to fall within the scope of these exemptions?
- Review and update website privacy policy if necessary
- Prepare data inventory and document compliance
- Prepare data protection assessments if necessary
- Implement internal process for compliance and handling consumer data access requests
- Written Information Security Program
- Review and update your vendor and service provider agreements