Wisconsin Legislative Council
STUDY COMMITTEE MEMO

Memo No. 1

TO: MEMBERS OF THE STUDY COMMITTEE ON THE USE OF ARTIFICIAL INTELLIGENCE IN HEALTH CARE

FROM: Margit Kelley, Principal Attorney, and Emily Hicks and Patrick Ward, Senior Staff Attorneys

RE: Overview of “Sandbox” Models; Wisconsin Bills Relating to Consumer Data Privacy and Artificial Intelligence; and Other States’ Definitions of “Artificial Intelligence”

DATE: September 2, 2026

During the August 13, 2026, meeting of the Study Committee on the Use of Artificial Intelligence in Health Care, members requested information from committee staff on “sandbox” models of state regulation of artificial intelligence (AI), as well as on consumer data privacy legislation and AI-specific health care legislation that was introduced in Wisconsin during the 2025-26 legislative session. Committee members also requested information from the National Conference of State Legislatures (NCSL) regarding other states’ definitions of “artificial intelligence.” This memo provides information in response to these requests.

SANDBOX MODELS

In the context of computer programming, a “sandbox” refers to a controlled environment in which applications can be tested without affecting existing operations. In the context of governmental regulations, a state regulatory sandbox tends to be structured as a program that provides developers with temporary relief from specified state laws or regulations while an application is tested or deployed under the oversight of a state entity. Testing under a state regulatory sandbox is usually done in the real world, rather than a controlled environment.[1]

As an example, Utah’s sandbox, the AI Learning Laboratory, is overseen by its Office of Artificial Intelligence Policy (OAIP) in the state’s Department of Commerce. [Utah Code Ann. ss. 13-72-201 and 13-72-301.] OAIP grants Learning Laboratory participants regulatory relief by negotiating and entering into “regulatory mitigation agreements” or joint interpretation agreements with them. These agreements must contain all of the following items:

- Limitations on scope of the use of the participant’s AI technology, which may include any of the following:
  - The number and types of users.
  - Geographic limitations.

[1] For additional resources regarding sandbox models, see Lucy Orr-Ewing, *Regulatory Sandbox Playbook*, Coalition for Health AI (Aug. 2026); and Randi Seigel, Jared Augenstein, and Maya Shashoua, *Testing the Future of AI: What AI Sandboxes Means for Innovation in Health Care*, Manatt (Feb. 3, 2026).

    - Other limitations to implementation.
- Safeguards to be implemented.
- Any regulatory mitigation granted to the applicant.
- Any required disclosures to consumers.
- Reporting requirements to comply with audits from OAIP.

[Utah Code Ann. s. 13-72-401 (4).]

To be eligible to participate in the Learning Laboratory, a developer must demonstrate all of the following statutory criteria:

- The participant has the technical expertise and capability to responsibly develop, implement, and use or supervise the use of the proposed AI technology.
- The participant has sufficient financial resources to meet obligations during testing.
- The AI technology provides potential substantial consumer benefits that may outweigh identified risks from mitigated enforcement of regulations.
- The participant has an effective plan to monitor and minimize identified risks from testing.
- The scale, scope, and duration of the proposed testing is appropriately limited based on risk assessments.

[Utah Code Ann. s. 13-72-402.]

OAIP has established "evidentiary expectations" that outline the office's goals of safeguarding patient safety and clinical function quality while balancing technological innovation with structured, measurable, and evidence-based clinical evaluation. The expectations identify core requirements for clinical competency, continuous quality assurance, and public health benefits.

In developing an agreement, OAIP must consult with relevant state agencies and entities regarding appropriate terms. Additionally, while an agreement is in effect, OAIP must perform regular audits of a participant's application of AI technology. OAIP may terminate an agreement at any time and for any reason. [Utah Code Ann. s. 13-72-401 (5), (6), and (8) (a).]

In October 2025, OAIP entered into a regulatory mitigation agreement with Doctronic, LLC, for an AI application that authorizes the renewal of certain verified prescriptions.[2] Under that agreement, OAIP and the Utah Division of Professional Licensing agreed to forgo certain enforcement actions against Doctronic and providers that use Doctronic, if the system is used within the designated parameters; specifically, the governmental parties agreed to forgo enforcement actions relating to Utah's laws prohibiting the unlicensed practice of certain professions and Utah's telemedicine laws for the duration of the agreement. In return, Doctronic is required to adhere to certain telehealth provider requirements and abide by agreed-upon procedures and safety protocols.

OAIP has entered into additional regulatory mitigation agreements with several companies, including Legion Health AI, an AI-enabled psychiatry clinic, to provide prescription refills of noncontrolled

[2] The Doctronic Regulation Mitigation Agreement applies to 192 medications, listed in Schedule C of the agreement. In a separate policy memorandum, the OAIP describes the formulary as comprising commonly prescribed maintenance medications and states specifically that it does not include controlled substances, injectables, drugs requiring routine laboratory monitoring, or short-course antibiotics.

substances for stable patients; ElizaChat, a pilot for AI-supported mental health access; and Dentacor, which provides AI-assisted analyses of dental radiographs at mobile clinics for low-income populations.

Select Legislation Introduced in Wisconsin in the 2025-26 Legislative Session

Consumer Data Privacy

Companion bills 2025 Senate Bill 166 and Assembly Bill 172 give a consumer certain rights over a person's personal data and impose certain obligations on any controller and processor of personal data.[3]

Applicability

The bills apply to a person who conducts business in Wisconsin or produces products or services that are targeted to residents of Wisconsin that meets either of the following conditions: (1) during a calendar year, the business controls or processes the personal data of at least 100,000 consumers; or (2) the business controls or processes personal data of at least 25,000 consumers and derives over 50 percent of its gross revenue from the sale of personal data. The bills specifically do not apply to listed organizations;[4] listed data, including certain data governed by federal law;[5] and deidentified data.[6]

The bills define "personal data" as any information that is linked or reasonably linkable to an identified or identifiable individual, but does not include deidentified data or publicly available information.

Consumers

The bills define a "consumer" as an individual who is a resident of Wisconsin, acting only in an individual or household context, and specifically do not include an individual acting in a commercial or employment context. Under the bills, a consumer has to the right to do any of the following:

- Confirm whether or not a controller is processing their personal data and to access such data.
- Correct inaccuracies in their collected personal data.

---

[3] For a comparison tool on other states' consumer data privacy laws, see Stauss, PLLC, *U.S. State Privacy and AI Resource Center (SPARC)* (last visited Aug. 25, 2026).

[4] The listed entities exempt from the bills are government entities; financial institutions or their affiliates subject to Title V of the federal Gram-Leach-Bliley Act; covered entities or business associates governed by the Health Insurance Portability and Accountability Act (HIPAA) or Health Information Technology for Economic and Clinical Health (HITECH) Act; nonprofit organizations; institutions of higher education; state agencies or political subdivisions of Wisconsin, including agents and entities that use public safety technologies for the purposes of bona fide law enforcement investigation; the entity under contract under s. 153.05 (2m), Stats., and its contractors; and the data organization under contract under s. 153.05 (2r), Stats., and its contractors.

[5] Some of the data exempted from the bills' requirements include health care information or records governed by HIPAA, HITECH, the Cures Act, or other similar laws; health care information protected by state statute; information created for purposes of the Health Care Quality Improvement Act; patient safety work product for the purposes of the Patient Safety and Quality Improvement Act; personal information on credit worthiness protected by the Fair Credit Reporting Act; personal data regulated by the Family Educational Rights and Privacy Act; and personal data regulated by the Farm Credit Act.

[6] The bills define "deidentified data" as data that cannot be reasonably linked to an identified or identifiable individual, or a device linked to such a person.

- Delete personal data provided by or obtained about them.
- Obtain a copy of their personal data that is portable.
- Opt out of the processing of personal data for targeted advertising, sale, or profiling.

A consumer can enforce these rights by making a request to a data controller, who must respond within 45 days and have a mechanism for a consumer to appeal their response.

Controllers

The bills define a "controller" as a person that, alone or jointly with others, determines the purpose and means of processing personal data. Under the bills, a controller must abide by the following rules:

- The controller must limit the collection of personal data to what is adequate, relevant, and reasonably necessary.
- The controller cannot process data for purposes that are not reasonably necessary and not compatible with the disclosed purposes for processing data.
- The controller must maintain reasonable data security practices.
- The controller cannot discriminate against a consumer who is exercising their rights under the bill, except for offering different prices, quality, or selection based on the consumer opting out of data collection or participation in a rewards program.
- The controller cannot process sensitive data without a consumer's consent.
- The controller must provide the consumer with a reasonably accessible, clear, and meaningful privacy notice.
- The controller must conspicuously disclose if they sell personal data to third parties for targeted advertising.

A controller must also conduct data protection assessments, which are further defined in the bill.

Processors

The bills define a "processor" as an individual or person that processes personal data on behalf of a controller. Under the bills, a processor must adhere to the directions of a controller and assist a controller in meeting the requirements of the bills, including responding to consumer rights requests, maintaining the security of personal data, and conducting data protection assessments. The bills require the contractual agreement between a controller and processor to address the following:

- Ensure each person processing personal data is subject to a duty of confidentiality.
- State that the processor must delete or return all personal data to the controller as requested.
- State that the processor must make the controller aware of the processor's compliance with the bills' requirements.
- State that the processor must either allow reasonable assessments by the controller or arrange for a qualified and independent assessor to conduct assessments of the processor's compliance with the bills.

Enforcement

As with other consumer protections under state law, the bills empower both the Department of Agriculture, Trade and Consumer Protection (DATCP) and the Department of Justice (DOJ) to enforce the bills' provisions and to serve subpoenas, complaints, orders, and other demands. Both DATCP and DOJ must give an entity 30 days written notice of potential violations. If within 30 days a controller or processor cures the noticed violation and provides DATCP or DOJ an express written statement that the alleged violations have been cured and no further violations will occur, no action for statutory damages can be initiated. However, if a controller or processor continues the violation, DATCP or DOJ may initiate an action and seek an injunction; civil forfeiture of no less than $100, but no more than $10,000 for each violation; recovery of reasonable expenses incurred; and, if appropriate, damages.

The bills do not create a private right of action.

History

On January 21, 2026, the Assembly Committee on Consumer Protection held a hearing on Assembly Bill 172 and received [written testimony on the bill](). On January 28, 2026, the committee voted to recommend passage of the bill on a vote of Ayes; 10; Noes, 0. On January 27, 2026, the Senate Committee on Licensing, Regulatory Reform, State and Federal Affairs held a public hearing on Senate Bill 166 and received [written testimony on the bill](); the committee did not hold a vote on whether to recommend passage of the bill. No further action was taken on either bill.

Insurers' Human-in-the-Loop

Companion bills [2025 Senate Bill 1066]() and [Assembly Bill 1109]() specify that a health insurer or self-insured governmental health plan may not use AI to deny a prior authorization for medical necessity or experimental status. An appropriate, licensed, individual health care practitioner must review a prior authorization request prior to denial. The bills do not define "artificial intelligence."

On March 4, 2026, the Senate Committee on Utilities, Technology and Tourism held a public hearing on Senate Bill 1066 and received [written testimony on the bill](). The companion, Assembly Bill 1109, did not receive a public hearing. The respective committees in the Senate and Assembly did not hold a vote on whether to recommend passage of the companion bills and no further action was taken.

Insurers' Disclosure of AI Use

Companion bills [2025 Senate Bill 1097]() and [Assembly Bill 1128]() create an Office of the Public Intervenor within the Office of the Commissioner of Insurance and require insurers to follow certain processes related to health insurance claims. The bills do not define "artificial intelligence." Specific to AI, the bills require an insurer to notify the insured if the insurer uses AI or algorithmic decision-making (ADM) to process a claim under a health insurance policy.

The notice must be in writing and must include all of the following items:

- A disclosure that AI or ADM was used in reviewing the claim, even if the outcome was reviewed by a human.
- A detailed explanation of how the AI or ADM reached its decision, including any factors the AI or ADM weighed.
- A contact point for requesting a human to review the claim if the claim was denied.

In addition to other reporting requirements, the bills require insurers that use AI or ADM in claims processing to annually publish a report detailing all of the following for the previous year for all health insurance policies under which the insurer provides coverage:

- The percentage of claims submitted to the insurer that were reviewed by AI or ADM.
- The claim denial rate of claims reviewed by AI or ADM compared to the claim denial rate of claims reviewed by humans.
- The steps the insurer takes to ensure fairness and accuracy in decisions made by AI or ADM.

Neither Senate Bill 1097 nor Assembly Bill 1128 received a public hearing in either house and no action was taken on either bill.[7]

Companion Chatbots for Minors

Companion bills 2025 Senate Bill 939 and Assembly Bill 965 prohibit a companion chatbot operator from making the companion chatbot available to a child unless it incorporates safety measures to prevent certain types of communication.

"Companion Chatbot" and "Artificial Intelligence" Definitions

Under the bills, a "companion chatbot" means a generative AI system with a natural language interface that simulates a sustained humanlike relationship with a user by doing all of the following:

- Retaining information on prior interactions or user sessions and user preferences to personalize the interaction and facilitate ongoing engagement with the generative AI system.
- Asking unprompted or unsolicited emotion-based questions that go beyond a direct response to a user prompt.
- Sustaining an ongoing dialogue concerning matters personal to the user.[8]

The bills define "artificial intelligence" as an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments.

Required Safety Features When a Companion Chatbot is Made Available to a Child

Under the bills, an operator may make a companion chatbot available to an individual that the operator reasonably determines is a child only if the companion chatbot incorporates safety measures to prevent all of the following:

- Encouraging a child to engage in self-harm, suicidal ideation, violence, consumption of drugs or alcohol, or disordered eating.
- Offering mental health services to a child or discouraging the child from seeking help from a qualified professional or appropriate adult.

---

[7] A similar provision was included in the Governor's proposed biennial budget bill, companion bills 2025 Senate Bill 45, SEC. 2887 and Assembly Bill 50, SEC. 2887.

[8] The bills exclude certain types of systems from the term "companion chatbot," including those used by a business entity for customer service, internal purposes, or employee productivity, or those solely designed and marketed for providing efficiency improvements or research or technical assistance.

- Encouraging a child to harm others or to participate in illegal activity, including the creation of child sexual abuse materials.
- Depicting or describing sexually explicit conduct to a child or soliciting depictions or descriptions of sexually explicit conduct from a child.
- Prioritizing validation of a child's beliefs, preferences, or desires over factual accuracy or a child's safety.
- Optimizing engagement in a manner that supersedes any of the above-listed safety measures.

History

On February 4, 2026, the Assembly Committee on Science, Technology, and AI held a public hearing on Assembly Bill 965 and received written testimony on the bill. The companion, Senate Bill 939, did not receive a public hearing. The respective committees in the Senate and Assembly did not hold a vote on whether to recommend passage of the companion bills and no further action was taken.

Other States' Definitions of "Artificial Intelligence"

In response to a request for a comparison of other states' definitions of "artificial intelligence," NCSL has provided a link to their web page, "State Artificial Intelligence (AI) and Related Terms Definition Examples," which includes a table that lists the definitions each state has, if any, for "artificial intelligence" and other related terms. Regarding common themes and variations in state definitions, NCSL notes the following:

> State definitions of artificial intelligence vary in both scope and approach. Most jurisdictions define AI as a machine-based system that can generate outputs such as predictions, recommendations or decisions and may influence physical or virtual environments. Some states adopt broad definitions focused on cognitive capabilities and autonomous operation, while others use narrower, application-specific definitions that address technologies such as generative AI or conversational systems.

MSK:EH:PW:kp