STATE OF WISCONSIN
Department of Employee Trust Funds
A. John Voelker
SECRETARY

Wisconsin Department
of Employee Trust Funds
PO Box 7931
Madison WI 53707-7931
1-877-533-5020 (toll free)
Fax 608-267-4549
etf.wi.gov

Correspondence Memorandum

Date: July 19, 2024

To: Group Insurance Board

From: Diana M. Felsmann, General Counsel
Office of Legal Services

Subject: Healthcare Legal Update

This memo is for informational purposes only. No Board action is required.

The purpose of this memo is to provide the Group Insurance Board (Board) a brief update on noteworthy healthcare-related legal updates, including a summary of relevant nationwide litigation.

Federal Trade Commission Lawsuit Against Pharmacy Benefits Managers
The Federal Trade Commission (FTC) is expected to file a lawsuit against the three biggest pharmacy benefits managers (PBMs) — UnitedHealth Group's Optum Rx, CVS Health's Caremark and Cigna's Express Scripts — over allegations that their tactics in negotiating prices for drugs, including insulin, dramatically increase costs to consumers and provide the PBMs with significant rebates.[1]

The announcement of imminent litigation by the FTC against these PBMs occurred on July 10, the day after the FTC issued an extensive interim report[2] on its study into PBM misconduct toward independent pharmacies and consumers.

Change Healthcare Breach
Change Healthcare runs the nation's largest electronic data clearinghouse used by thousands of providers, pharmacies, and insurers to verify insurance, confirm pre-authorizations, and exchange insurance claims data. UnitedHealth Group acquired Change Healthcare in 2022.

As discussed at previous Board meetings, on Feb. 21, 2024, Change Healthcare identified that it had been the subject of a cyberattack of unprecedented magnitude in

---

1 https://www.wsj.com/health/pharma/ftc-to-sue-drug-managers-over-insulin-prices-b46af71f
2 https://www.ftc.gov/system/files/ftc_gov/pdf/pharmacy-benefit-managers-staff-report.pdf

Reviewed and approved by John Voelker, Secretary
Electronically Signed 07/25/2024

Board	Mtg Date	Item #
GIB	08.14.24	13A

the healthcare industry. In his testimony in front of the federal House Committee on Energy and Commerce, the UnitedHealth CEO indicated that the breach, caused by compromised credentials and a lack of multi-factor authentication, exposed the sensitive information of about one-third of Americans.[3]

At last count, 50 lawsuits had been filed against Change Healthcare based on this breach. On June 7, 2024, those 50 cases were consolidated into a single class action in the federal district court of Minnesota.[4] The consolidated case currently involves individuals whose personally identifiable information or Health Insurance Portability and Accountability Act (HIPAA)-protected health information was exposed during the breach. The case also includes a number of healthcare providers who say that they were unable to get paid when Change Healthcare's systems were locked down after the cyberattack.

In addition to this class action, the federal Health and Human Services Office for Civil Rights (OCR) has opened breach investigations into Change Healthcare and UnitedHealth Group, focusing on whether a HIPAA breach occurred and on their overall compliance with HIPAA. OCR is the federal entity that enforces HIPAA.[5]

Ozempic, Wegovy, Rybelsus, Mounjaro, and Trulicity Consolidated Litigation

- In February of 2024, 55 individual cases brought against Novo Nordisk or Eli Lilly over side effects from glucagon-like peptide-1 receptor agonists (GLP-1 RA) were consolidated into one multi-district litigation[6] in the eastern district of Pennsylvania.[7] Novo Nordisk is the maker of Ozempic, Wegovy, and Rybelsus, and Eli Lilly manufacturers Mounjaro and Trulicity. The number of cases grew from 55 to 88 in May and is expected to increase into the thousands.

Plaintiffs allege that they were not sufficiently warned of significant side effects from taking GLP-1 RA's, including gastroparesis, ileus, intestinal obstruction or pseudo-obstruction, some form of gallbladder injury, or other gastrointestinal injury. Novo Nordisk and Eli Lilly have responded that the known risks are identified in FDA-approved product labeling, certain plaintiffs lack a specific diagnosis, and it is possible that some of the plaintiffs may have been taking counterfeit products.

---

[3] https://d1dth6e84htgma.cloudfront.net/Witty_Testimony_OI_Hearing_05_01_24_5ff52a2d11.pdf

[4] https://fingfx.thomsonreuters.com/gfx/legaldocs/zgvonrbaqpd/Change%20Healthcare%20MDL%20order%206-7.pdf

[5] https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html

[6] 28 U.S.C. Section 1407 provides for multi-district litigation which permits the temporary transfer of federal lawsuits to one or more federal district courts for pre-trial consolidation or coordination. Multi-district litigation is different than a class action lawsuit. Multi-district litigation is often used when individuals claim to have been injured by the same medications, but their individual reactions varied.

[7] *In re: Glucagon-Like Peptide-1 Receptor Agonists (GLP-1 RAS)* Products Liability Litigation, Case No. MDL-3094 (E.D. Pa)

Artificial Intelligence and Claims Determinations
In separate legal cases, UnitedHealth and Humana have both been accused of using a flawed artificial intelligence (AI) algorithm to deny post-acute care claims of Medicare Advantage plan participants. Cigna has also been accused of using AI software to routinely deny claims without reviewing patient files.

In the UnitedHealth case,[8] plaintiffs argued that its “nH Predict” algorithm resulted in the routine denial of post-acute care. They further allege that about 90% of those denials were overturned on appeal. In May, UnitedHealth filed a motion to dismiss the case, arguing, among other things, that the plaintiffs failed to exhaust the Medicare administrative appeals process.

The Humana case[9] similarly involves the use of nH Predict in claims denials for Medicare Advantage claims.

In the Cigna lawsuit,[10] plaintiffs alleged that Cigna used AI to automatically deny over 300,000 patient claims without reviewing their files. Specifically, they asserted that Cigna’s software system approved and denied claims in batches, spending an average of 1.2 second on each claim. Cigna has moved to dismiss the case, asserting that it uses technology to verify codes on some common, low-cost procedures to expedite physician reimbursement.

In other AI news, members of Congress sent a letter[11] on June 25, 2024, to the Centers for Medicare & Medicaid Services (CMS) urging them to proceed with caution and increase oversight with respect to the use of AI for Medicare Advantage coverage determinations. The legislators asked CMS to issue more detailed guidance and prohibit the use of AI and algorithmic tools in coverage denials until a systematic review of their use is completed.

CVS’ Alleged Failure to Effectively Forecast Medical Cost Trends and Healthcare Utilization
On July 12, 2024, a securities-proposed class action was filed on behalf of CVS shareholders alleging that CVS failed to effectively forecast medical cost trends and health care utilization patterns.[12] According to the complaint, the outcome of those failures was ultimately a decrease in profitability because CVS did not change enough in plan premiums.

---

[8] *Estate of Gene B. Lokken v. UnitedHealth Group Inc.*, 23-CV-03514 (D. Minn.), https://aboutblaw.com/bbs8
[9] *Barrows v. Humana, Inc.*, 3:23-cv-00654-RGJ (W.D. K.y) https://aboutblaw.com/bbRX
[10] *Kisting-Leung v. Cigna Corp*., 2:23-cv-01477, (E.D. Cal.) https://aboutblaw.com/9vN
[11] https://chu.house.gov/sites/evo-subsites/chu.house.gov/files/evo-media-document/Final%20Chu-Nadler-Warren%20Letter%20to%20CMS%20to%20Increase%20Oversight%20of%20AI%20in%20Medicare%20Advantage%20Coverage%20Decisions%2006.25.2024.pdf
[12] 24-cv-05303(S.D.N.Y.)

End of *Chevron* Deference

Courts no longer need to defer to reasonable federal agency interpretations of ambiguous statutes. Specifically, on June 28, 2024, the United States Supreme Court issued a consolidated opinion in *Loper Bright Enterprises v. Raimondo* and *Relentless, Inc. v. Department of Commerce* (*Loper Bright*), overruling the doctrine of "*Chevron* deference" based on a 1984 United States Supreme Court decision of the same name.[13]

The *Loper Bright* decision explicitly stated that it did not call into question previous cases that were based on *Chevron*. Going forward, however, courts reviewing federal agency actions, including CMS or federal Health and Human Services regulations, must determine a statute's "single best meaning." Courts may still consider federal agency interpretations, with greater weight given to interpretations issued contemporaneously with the statutory language and that have remained consistent over time.

Loper Bright will likely make federal agencies more cautious in their rulemaking, guidance and policies. It may also cause an increase in litigation as individuals question whether a federal agency has exceeded its authority.

Cybersecurity and the Fiduciary Duty of Prudence

The American Retirement Association recently interviewed Lisa Gomez, Assistant Secretary of Labor for the Employee Benefits Security Administration (EBSA) at the United States Department of Labor (DOL) about cybersecurity.[14] During the interview, Assistant Secretary Gomez emphasized that plans should focus on the fiduciary duty of prudence concerning all aspects of a plan, whether the issue is cybersecurity overall, AI, or cyber liability insurance.

Gomez also referenced DOL's 2021 cybersecurity best practices[15] and how they offer plans guidance on robust, measurable cybersecurity protections.

Staff will be at the Board meeting to answer any questions.

[13] *Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.*, 468 U.S. 837 (1984).
[14] Exclusive: A Candid Cybersecurity Conversation with EBSA's Lisa Gomez | National Association of Plan Advisors (napa-net.org)
[15] https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf