IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

ELLSWORTH WILLIAM JEFFRIES, III, et al., Plaintiffs, v. HARCROS CHEMICALS INC., et al., Defendants.	Case No. 25-2352-KHV-ADM

VANESSA TUCKER, individually and on behalf of those similarly situated, Plaintiff, v. HARCROS CHEMICALS INC., et al., Defendants.	Case No. 25-2569-KHV-ADM

MEMORANDUM AND ORDER

These consolidated cases are putative class actions brought by plaintiffs who live within a three-mile radius of a chemical facility in Kansas City, Kansas. Plaintiffs contend this facility has emitted a "toxic cocktail" of emissions that have poisoned and contaminated the air, leading to severe and chronic injuries to residents in the surrounding vicinity. Defendants are a series of entities that collectively owned and operated the facility over a period of several decades, including Harcros Chemicals, Inc. ("Harcros"), Philips North America LLC f/k/a Philips Electronics North America Corporation and Koninklijke Phillips N.V. ("Philips"), and Elementis Chemicals, Inc. ("Elementis"). This case is now before the court on Defendants' Motion to Amend the Protective

Order that the court has already entered to govern discovery in this case. (ECF 120.) For the reasons explained below, Defendants' motion is granted.

I. BACKGROUND

When the court originally entered the protective order in this case (ECF 115), the court resolved the parties' first round of disputes over restrictions for using AI Tools in relation to Confidential Information. The protective order provides, among other things, that a party intending to use a particular AI Tool must provide other parties with notice and an opportunity to object; ensure that the AI Tool is used in a secure environment and that Confidential Information is not used to train or improve any AI Tool except one used exclusively in this action; to the extent that an AI Tool is trained or improved using Confidential Information, that information is destroyed at the conclusion of this litigation and is not made accessible to anyone not authorized to have access to Confidential Information; and ensure that all Confidential Information is deleted at the conclusion of this action. (*Id.* ¶ 8, at 6-8.) As a practical matter, these provisions effectively require parties to use only closed or secure AI Tools ("closed AI Tools") for Confidential Information. At the time the court entered the protective order, the parties foreshadowed a broader dispute over the use of AI Tools in connection with *all* information produced in discovery in this case, not just Confidential Information.

The parties have further crystallized their dispute on this point, which is now before the court on Defendants' Motion to Amend the Protective Order. (ECF 120.) By way of this motion, Defendants seek to amend the protective order language to expand the AI provisions described above to apply not only to documents and information designated as "Confidential," but more broadly to all "Discovery Materials"—*i.e.*, all documents and information produced in discovery. Highly summarized, Defendants seek to prevent parties from uploading even non-confidential

documents into public or "open loop" generative artificial intelligence tools (collectively, "open AI Tools").

For the reasons stated below, the court finds good cause to enter the amended version of the protective order proposed by Defendants. The court therefore grants Defendants' motion and enters an Amended Protective Order in line with the proposed protective order attached to Defendants' motion (ECF 120-1).

II. LEGAL STANDARD

Under Federal Rule of Civil Procedure 26(c)(1), the court may, for good cause, "issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense." Rule 26(c)(1) permits a court to issue a protective order "limiting the scope of disclosure or discovery to certain matters." *See* FED. R. CIV. P. 26(c)(1)(D). Rule 26(c)(1)'s good-cause standard is "highly flexible, having been designed to accommodate all relevant interests as they arise." *Rohrbough v. Harris*, 549 F.3d 1313, 1321 (10th Cir. 2008).

III. ANALYSIS

Defendants assert that good cause exists for their proposed amendment governing the disclosure of non-confidential materials because the availability and use of AI Tools in litigation "represents a paradigm shift of yet-to-be defined proportions, but what is clear is that the way AI Tools function poses a potential threat to the integrity and security of data produced in litigation." (ECF 120, at 2.) Defendants explain that AI Tools rely on sophisticated machine learning models that work by identifying and encoding patterns and relationships in massive amounts of data and then using that information to understand users' natural language requests or questions and respond with relevant new content. But, unlike closed AI Tools, the use of open AI Tools "risks disclosure, loss of control, and uncertainty concerning the security, storage, and other data-handling of that

information." (*Id.* at 2-3.) Defendants point out that, because an open AI Tool uses the data submitted to it to continually develop and improve the tool, it is "practically impossible" to claw back data later determined to be privileged, or delete data from the open AI Tool at the conclusion of the action (as required by the deletion clause in the Protective Order) because the information was used to train the AI Tool. (*Id.* at 3, 6-7.) Defendants further explain the harm that might result if information cannot be clawed back or deleted—*e.g.*, waiving confidentiality or privilege of information that was inadvertently disclosed without a "confidential" designation; revealing sensitive data or personal information from the AI Tool's training datasets; and potentially violating counsel's professional duty to safeguard information relating to representation of a client. (*Id.* at 3-5.) Defendants also point out that wholesale submission of discovery materials to an open AI Tool may violate U.S. data privacy laws and the strict disclosure rules under the European General Data Protection Regulation ("GDPR"), to which defendants Elementis and Philips are subject. (*Id.* at 7-8.) Lastly, Defendants contend that their proposed amendment is necessary to protect against exposure of critical infrastructure and data breach, given that Defendants are part of the chemical sector designated as Critical Infrastructure and vital to national security. (*Id.* at 8-9.) Defendants contend that all of these concerns constitute good cause to amend the protective order.

Plaintiffs dispute that Defendants have shown good cause for what Plaintiffs characterize as an "umbrella" protective order that is disfavored by courts. Plaintiffs also contend that Defendants' proposal would drive up Plaintiffs' costs by denying them access to open AI Tools to analyze "otherwise unprotected discovery materials." (ECF 123, at 5-6, 8.) Plaintiffs further argue that Defendants' proposal deprives Plaintiffs of their First Amendment right to use and disseminate nonconfidential discovery materials to public-use, open AI Tools. (*Id.* at 4, 5.) Lastly, Plaintiffs

say that Defendants' arguments regarding the impossibility of clawing back or deleting the documents submitted to an open AI Tool and regarding potential violations of privacy laws and the GDPR are only speculative. (*Id.* at 8-9.)

To begin, the court disagrees with Plaintiffs' characterization of Defendants' proposal as a disfavored "umbrella" protective order. Umbrella protective orders preemptively designate all discovery as protected without any review by either the court or the parties. *See Mann v. Con-Way Freight*, No. 16-2196-CM-JPO, 2016 WL 6164013, at *4 (D. Kan. Oct. 24, 2016) (citation omitted). Although Defendants' proposed protective order covers all discovery materials, the parties will still be reviewing and screening discovery materials to determine the extent to which they should be marked "Confidential." So, Defendants are not proposing the type of "umbrella" protective order that is disfavored by the courts.

The court turns next to Plaintiffs' contention that Defendants' proposal seeks to increase Plaintiffs' litigation costs by depriving them of open AI Tools to analyze discovery materials and making it more burdensome for Plaintiffs to pursue this litigation. (ECF 123, at 5.) Plaintiffs have not presented any support for the increased burden, such as by attempting to quantify the extent of any such increased cost. Thus, the court does not find that Plaintiffs would suffer an *undue* burden if the court were to grant Defendants' motion. Indeed, Plaintiffs and their attorneys initiated this lawsuit knowing that class action litigation is expensive, including the costs of eDiscovery, expert witness fees, and administrative, court-filing, and other expenses. And, as Defendants point out, their proposal "applies equally to all parties and allows all parties to use Closed AI Tools that meet basic security requirements," thereby putting the same financial burden on Plaintiffs and Defendants. (ECF 129, at 1.)

Next, the court turns to Plaintiffs' contention that Defendants' proposed amended protective order deprives Plaintiffs of their First Amendment right to use and disseminate nonconfidential discovery materials. Not so. A protective order does not offend the First Amendment when it is entered based on a showing of good cause, is limited to the context of pretrial civil discovery, and does not restrict the dissemination of the information if gained from other sources. *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 37 (1984). Here, Defendants' proposed amended protective order does not prohibit the parties from disseminating non-confidential documents to the public. Indeed, Defendants concede that their proposed amended protective order "does not in any respect affect how all parties—consistent with applicable law, ethical requirements, and professional standards—can publicize non-confidential documents by posting such documents to a website, making documents available to the media, or attaching documents to a court filing." (ECF 129, at 2-3.)

Lastly, the court addresses Plaintiffs' argument that Defendants have not met their burden to show the need for the relief sought. Plaintiffs point out that Defendants did not submit an affidavit from a cybersecurity expert to back up their claims of risk or to analyze the regulatory framework of the GDPR or provide specific examples of problematic discovery materials. Plaintiffs view Defendants' proposal as seeking to "convert all discovery into protected material . . . based on speculative fears untethered to any concrete showing of harm." (ECF 123, at 4, 5, 8-9.) In reply, Defendants point out that their motion presents an "issue of first impression" and call attention to the documents and policies they cited in their motion, which "establish the scrutiny and care that must be taken when submitting data, particularly that from within a critical infrastructure industry, to Public AI Tools" given the "AI-specific security risks that may expose training or other data." (ECF 129, at 3-4.)

On balance, Defendants have the better arguments. Plaintiffs never directly address Defendants' argument that clawing back or deleting data submitted to an open AI Tool is impossible as a practical matter because such data is used to continually develop and improve the tool. Nor do they address Defendants' argument that the use of an open AI Tool may expose Defendants' critical infrastructure information to cyber criminals and risk data breach. Instead, they just call the arguments "speculative" and insist that any resulting harm from the information's disclosure is no greater than if Plaintiffs publicly posted the nonconfidential information on a website, which the current version of the protective order would not prohibit. (ECF 123, at 8-9.) But this analogy is not persuasive. The use of widely available AI Tools presents the opportunity for a centralized repository that makes information available to the public at a scale that was not historically available and ignores the very real security risks of public AI Tools, including the inability to effectively claw back information from the AI Tool.

It is indisputable that generative AI may automate many time-consuming tasks in the eDiscovery process, such as significantly accelerating document review, quickly summarizing documents, streamlining privilege review and logging, identifying named entities like key people and organizations, extracting important topics, and automating writing tasks, such as drafting deposition questions, creating narrative timelines from evidence, and drafting legal briefs. But Defendants' proposal does not foreclose a party from using *any* AI Tools; it only prohibits using open AI Tools while allowing the use of closed AI Tools—for good reason. The wholesale submission of discovery materials to an open AI Tool for these eDiscovery tasks could expose massive amounts of data. These actions may violate U.S. data privacy laws and the stricter GDPR disclosure rules, which set a high standard for protecting individuals' information and requires documented consent to be "freely given, specific, informed and unambiguous." (GDPR Article

4(11).) As Defendants point out, Defendants' employees, contractors, and correspondents have not consented. Thus, Plaintiffs' proposal, which proposes only redaction of certain personally identifiable information, does not appear to comply with the strict requirements of the GDPR, including the consent requirement.

On balance, the court finds that Defendants have met their burden to show the need for the relief sought given the AI-specific risks identified by Defendants in this particular case—namely, where documents to be submitted to the AI Tool come from entities in a critical infrastructure industry and disclosure may violate data privacy laws. Plaintiffs' arguments do not persuade the court otherwise. Parties are often required to produce massive amounts of information in complex litigation, and this often includes documents that may include a small amount of information that is responsive to discovery requests amongst otherwise largely irrelevant or non-responsive information. *See, e.g.*, *Ritchie v. Wal-Mart Stores East, L.P.*, No. 19-4067-SAC-ADM, 2020 WL 5369392, at *2 (D. Kan. Sept. 8, 2020) ("Ordinarily, a party may not unilaterally redact information from documents it produces in litigation simply because the redacted information is irrelevant or non-responsive."). If the court were to allow a party to upload all non-confidential documents and materials produced by another party to an open AI Tool, thereby making all such data amenable to public consumption, parties may err on the side of under-producing potentially responsive documents or seek to make extensive redactions of irrelevant or non-responsive information. Defendants' proposed amendment allowing the use of closed AI Tools, as opposed to open AI Tools, will facilitate discovery by incentivizing more fulsome document productions.

IV. CONCLUSION

In conclusion, the court finds that Defendants have shown good cause for entry of Defendants' proposed amended protective order for the reasons stated above.

IT IS THEREFORE ORDERED that Defendants' Motion to Amend the Protective Order (ECF 120) is granted. The court will enter the Amended Protective Order forthwith.

IT IS SO ORDERED.

Dated March 25, 2026, at Kansas City, Kansas.

s/ Angel D. Mitchell
Angel D. Mitchell
U.S. Magistrate Judge