

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

TIWAN ALLEN, on behalf of herself and)
all others similarly situated,)

Plaintiff,)

v.)

MIDWEST EXPRESS CARE, INC. d/b/a)
MIDWEST EXPRESS CLINIC)

Defendant.)

Case No. 24-cv-05348

Judge Sharon Johnson Coleman

MEMORANDUM OPINION AND ORDER

Plaintiff Tiwan Allen, on behalf of herself and others similarly situated, (“Plaintiff”) filed her Complaint against Defendant Midwest Express Care, Inc. d/b/a Midwest Express Clinic (“Defendant”) alleging violations of the Electronic Communications Privacy Act, negligence and unjust enrichment.¹ Before the Court is Defendant’s Motion to Dismiss Plaintiff’s Complaint under Federal Rule of Civil Procedure 12(b)(6). For the following reasons, the Court denies Defendant’s Motion to Dismiss [27].

BACKGROUND

The following facts are accepted as true for the purpose of resolving Defendant’s Motion to Dismiss.

Defendant operates urgent care clinics throughout Illinois and Indiana. In 2019, Plaintiff became a patient of Defendant. In order to receive treatment, Plaintiff had to disclose her personally identifiable information (“PII”) and protected health information (“PHI”) to Defendant on numerous occasions, most recently in January 2024. Plaintiff alleges that she used Defendant’s website to request and book doctor’s appointments, search and communicate information concerning specific medical

¹ In Plaintiff’s response to the Motion to Dismiss, Plaintiff withdrew her Illinois Eavesdropping Statute claim.

conditions, her patient status, treatments sought, and locations where Plaintiff received healthcare treatment. Plaintiff alleges that Defendant installed Meta Pixel (“Pixel”), Google Analytics, and Google Tag Manager (together “Tracking Technologies”) on its website, which “allowed unauthorized third parties to intercept the contents of patient communications, view patients’ PII and PHI, mine the information for purposes unrelated to the provision of healthcare and further monetize it to deliver targeted ads, among other things.” Dkt. 1, at ¶ 8. Specifically, Plaintiff claims that Pixel “tracks the people and actions they take,” meaning when a user accesses a website that hosts Pixel, the user’s communications with the website are “instantaneously and surreptitiously duplicated and sent to Facebook’s servers.” Dkt. 1, at ¶ 33. These communications are linked and connected to the user’s Facebook profiles, enabling Facebook to identify the user that is conducting the website searches on Defendant’s webpage.

Since 2010, Plaintiff has maintained a Facebook account. Plaintiff alleges that she received targeted advertisements on Facebook or Instagram, inviting her to visit other Defendant clinic locations and advertisements related to the medical conditions she searched on Defendant’s website. Plaintiff claims that she received these advertisements because Defendant installed Pixel on its website.

On June 26, 2024, Plaintiff, on behalf of herself and others similarly situated, filed this lawsuit.

LEGAL STANDARD

A motion to dismiss pursuant to Rule 12(b)(6) for failure to state a claim tests the sufficiency of the complaint, not its merits. *See Camasta v. Jos. A. Bank Clothiers, Inc.*, 761 F.3d 732, 736 (7th Cir. 2014). When considering dismissal of a complaint, the Court accepts well pleaded factual allegations as true and draws all reasonable inferences in favor of the plaintiff. *Erickson v. Pardus*, 551 U.S. 89, 94, 127 S. Ct. 2197, 167 L. Ed. 2d 1081 (2007) (per curiam); *Trujillo v. Rockledge Furniture LLC*, 926 F.3d 395, 397 (7th Cir. 2019). To survive a motion to dismiss, plaintiff must “state a claim to relief that is plausible on its face.” *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570, 127 S. Ct. 1955, 167 L. Ed. 2d

929 (2007). A complaint is facially plausible when the plaintiff alleges “factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S. Ct. 1937, 173 L.Ed.2d 868 (2009).

DISCUSSION

I. Count I: Violations of the Electronic Communications Privacy Act

The Electronic Communications Privacy Act (the “ECPA”) forbids a person from “intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept, any wire, oral or electronic communication.” 18 U.S.C. § 2511(a). The ECPA requires a plaintiff to demonstrate that a defendant “(1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication, (5) using a device.” *Stein v. Edward-Elmhurst Health*, No. 23-cv-14515, 2025 WL 580556, at *3 (N.D. Ill. Feb. 21, 2025) (Seeger, J.). The ECPA has an exception to these requirements, known as the one-party consent rule exception. *See* 18 U.S.C. § 2511(d). The one-party consent rule exception holds that the ECPA is not violated where a party to the communications intercepts its own communications. *See id.* However, an “exception to the exception” exists where the party to the communication intercepts its own communication “for the purpose of committing any criminal or tortious act...” (the “Crime-Tort Exception”). *Id.* The Crime-Tort Exception only applies if the criminal or tortious act is independent of the interception of the communication itself. *See Stein*, 2025 WL 580556, at *4.

In sum, the ECPA makes it unlawful to intentionally intercept communications, unless it is a party to the communication, but the party cannot intercept the communication if it is for the purpose of committing a criminal or tortious act that is independent from the intentional interception of such communications.

Here, Plaintiff alleges that the Crime-Tort Exception applies because Defendant intercepted the communications for the purpose of violating the Health Insurance Portability and Accountability Act (“HIPPA”) by collecting her individually identifiable health information (“IIHI”) and disclosing her IIHI to third parties, such as Facebook.

Defendant first argues that the Crime-Tort Exception does not apply because it did not disclose Plaintiff’s IIHI. HIPPA imposes liability for knowingly “disclos[ing] [IIHI] to another person.” 42 U.S.C. § 1320d-6(a)(3). IIHI is any information that

(A) is created and received by a health care provider, health plan, employer, or health care clearinghouse; and (B) relates to the present, past, 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) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

42 U.S.C.A. § 1320d(6).

Here, Plaintiff alleges that Defendant implemented the Tracking Technologies on its website and sent non-public private information, including, but not limited to, Plaintiff’s status as a medical patient, health conditions, medical treatments, the specific locations where treatment was sought, and the particular words and phrases typed into the search bar on the website, including searches for treatment and information related to her medical conditions, to third parties, such as Facebook and Google. Dkt. 1, at ¶ 66. This information qualifies as IIHI and such disclosure, as alleged here, violates HIPAA. Many courts in this District have found the same to be true. *See Stein*, No. 23-cv-14515, 2025 WL 580556, at *6 (N.D. Ill. Feb. 21, 2025) (Seeger, J.) (finding that disclosure of health information to a third party is a violation of HIPPA); *A.D. v. Aspen Dental Management, Inc.*, No. 24 C 1404, 2024 WL 4119153, at *3 (N.D. Ill. Sept. 9, 2024) (Kendall, J.) (finding disclosure about patient status, medical conditions, information about medical appointments and treatments, and medical providers to qualify as IIHI for purposes of HIPAA); *Smith v. Loyola Univ. Med. Ctr.*, No. 23 CV 15828, 2024 WL 333891, at *7 (N.D. Ill. July 9, 2024) (Daniel, J.) (concluding that disclosure of personal

health information qualifies as IIHI for purposes of HIPPA); *Kurkowski v. Rush System for Health*, No. 22 C 5380, 2023 WL 8544084, at *3 (N.D. Ill. Dec. 11, 2023) (Kennelly, J.) (determining that the sharing of medical information was sufficient to invoke HIPPA).

Defendant next contends that the Crime-Tort Exception does not apply because Defendant did not intercept the communications for the purpose of committing a crime or tort, but for financial gain. Defendant heavily relies on *Desnick v. Am. Broad Companies, Inc.*, 44 F.3d 1345 (7th Cir. 1995) to support its position. In *Desnick*, the Seventh Circuit concluded that the Crime-Tort Exception did not apply where the defendant sent undercover testers into a doctor's office, later broadcasting the footage on television, because it did not do so for the purpose of defaming the plaintiffs, but to see whether the doctors would recommend unneeded cataract surgery. *Desnick*, 44 F.3d at 1353 ("Telling the world the truth about a Medicare fraud is hardly what the framers of the statute could have had in mind in forbidding a person to record his own conversations if he was trying to commit an 'injurious' act.")

Desnick is distinguishable from this case. Here, Defendant disclosed Plaintiff's IIHI and HIPAA imposes criminal liability for such disclosure. Even if Defendant argues that its motivation was for financial gain, the Court cannot separate such alleged motive from the reality that such revenue could only be gained by committing a HIPAA violation. In other words, Defendant had to commit a crime/tort under HIPAA, namely, the disclosure of Plaintiff's IIHI, to gain financial profit. The Court finds that this is enough to satisfy the Crime-Tort Exception at this time.

Lastly, Defendant argues that the Crime-Tort Exception does not apply because the criminal or tortious act is not separate and distinct from the alleged wiretap. Not only does Defendant cite to nonprecedential authority in support of this position, but Plaintiff properly alleges that Defendant intentionally violated HIPAA when it allowed Plaintiff's IIHI to be intercepted, disclosed, viewed, analyzed, and used by third parties, which is distinct from the improper interception in the ECPA claim. Dkt. 1, at ¶¶ 10, 186-188.

Accordingly, Defendant's motion to dismiss Count I is denied.

II. Count II: Negligence

To state a negligence claim, a plaintiff must show that (1) defendant owed a duty of care to plaintiff, (2) defendant breached that duty; and (3) defendant's breach was the proximate cause of plaintiff's injuries. *Cosgrove v. Commonwealth Edison Co.*, 315 Ill. App. 3d 651, 654 (2000). Defendant argues that Plaintiff fails to satisfy the first element of her negligence claim: that Defendant owed Plaintiff a duty. Specifically, Defendant contends that Illinois courts have not recognized a tort claim for breach of physician-patient confidentiality, and thus Defendant does not owe Plaintiff a duty as a medical provider. Plaintiff alleges that Defendant had a duty to safeguard her protected medical information and prevent disclosure of her personal health information.

Under Illinois' Personal Information Protection Act ("PIPA"), "[a] data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure." 815 ILCS 530/45. Illinois courts have found that, under PIPA, data collectors have a duty to maintain reasonable security measures. *See Smith*, 2024 WL 333891, at *7 (collecting cases).

Here, Plaintiff alleges that Defendant collected Plaintiff's non-public information and, thus, had a duty to maintain reasonable security measures to prevent the disclosure of Plaintiff's information. *See* Dkt. 1, at ¶ 59. Defendant contends that PIPA cannot support a negligence claim because the Illinois Supreme Court has expressed its hesitation to recognize a new tort where a statute, such as PIPA, provides a comprehensive scheme for remedying such tortious actions. However, as of the date of this Order, the Illinois Supreme Court has not spoken on whether PIPA can support a negligence claim. Federal district courts are not tasked with creating restrictions that state law does not recognize. *Stein*, 2025 WL 580556, at *9. We must take the law as it stands, not "break new

ground in state law.” *See Sabrina Roppo v. Travelers Com. Ins. Co.*, 869 F.3d 568, 598 (7th Cir. 2017) (internal quotations omitted).

Here, Plaintiff alleges that Defendant collected Plaintiff’s non-public health information and, thereafter, disclosed this information to unauthorized third parties without her consent. This is sufficient to plausibly allege duty to state a negligence claim.

Accordingly, Defendant’s motion to dismiss Count II is denied.

III. Count III: Unjust Enrichment

Under Illinois law, to state a claim for unjust enrichment, a plaintiff must allege that “the defendant has unjustly retained a benefit to the plaintiff’s detriment, and that defendant’s retention of the benefit violates the fundamental principles of justice, equity, and good conscience.” *Control Solutions LLC v. Oshkosh Corp.*, No. 10 C 121, 2012 WL 3096678, at *10 (N.D. Ill. 2012) (Coleman, J.) (internal citations omitted). As the Court denied Defendant’s motion to dismiss Counts I and II, Defendant’s remaining argument is that Plaintiff fails to state a claim for unjust enrichment because she failed to allege that she had any plans to monetize the information she provided to Defendant and that courts have routinely rejected the proposition that PII has any independent monetary value.

In support of its position, Defendant cites *In re Arthur J. Gallagher Data Breach Litig.*, 631 F.Supp.3d 573 (N.D. Ill. 2022) (Rowland, J.) However, the Court finds this case inapplicable. *In re Arthur J. Gallagher Data Breach Litig.* concerned claims stemming from a data breach that resulted in the unauthorized disclosure of plaintiffs’ PII, such as their names, social security numbers, tax ID numbers, driver’s license, and government IDs, to name a few. 631 F.Supp.3d at 581. In ruling on the unjust enrichment claim, the court found that plaintiffs failed to plead unjust enrichment because there was no independent monetary value of plaintiff’s PII. *Id.* at 592.

Here, however, Plaintiff pleads that Defendant was motivated by financial profit when it disclosed Plaintiff’s PHI and PII to unauthorized third parties. Unlike *In re Arthur J. Gallagher Data*

Breach Litig., where the disclosure was caused by a data breach, Plaintiff alleges that Defendant intentionally disclosed Plaintiff's PHI and PII for monetary benefit. As pled, the disclosure of the PHI and PII was tied to financial profit. This is enough to adequately plead unjust enrichment at the motion to dismiss stage.

Accordingly, the Court denies Defendant's motion to dismiss Count III.


CONCLUSION

For these reasons, the Court denies Defendant's Motion to Dismiss in total [27].

IT IS SO ORDERED.

Date: 8/6/2025

Entered: _____


SHARON JOHNSON COLEMAN
United States District Judge