IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

NATALIE BRAHM,

Plaintiff,

v.

HOSPITAL SISTERS HEALTH SYSTEM and SACRED HEART HOSPITAL OF THE HOSPITAL SISTERS OF THE THIRD ORDER OF ST. FRANCIS,

Defendants.

OPINION AND ORDER

23-cv-444-wmc

Plaintiff Natalie Brahm originally filed this proposed class action lawsuit in the Circuit Court for Eau Claire County, Wisconsin, claiming that the defendants -- Hospital Sisters Health System and Sacred Heart Hospital of the Hospital Sisters of the Third Order of St. Francis (collectively, "Hospital Sisters") -- routinely disclose patients' identities and protected health care information obtained when they visit the defendants' website through advertising technology referred to as "pixel tracking," then share that information with third party advertising websites, including Facebook and Google, all without their patients' consent or knowledge in violation of various Wisconsin common and statutory law. Defendants removed the lawsuit to this court under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d),[1] and moved to dismiss, arguing that plaintiff fails to state

[1] Plaintiff has not challenged removal and, to date, has not disputed this court's exercise of subject matter jurisdiction under CAFA. Moreover, the proposed class size appears to exceed 100; minimal diversity is satisfied as to plaintiff and at least one of the two defendants; and a good faith estimate of the amount in controversy exceeds $5 million. *See* 28 U.S.C. §§ 1441, 1446, 1332(d), and 1453(b). Accordingly, the court is satisfied that the jurisdictional requirements are met consistent with defendants' representations in their notice of removal. (Dkt. #1.) Specifically, plaintiff represents (and the court has no basis to question) that: the proposed class consists of thousands of members; plaintiff and defendant Hospital Sisters Health System are citizens of different states;

any claim upon which relief may be granted. (Dkt. #16.) For the reasons that follow, the court will grant defendants' motion with respect to plaintiff's claim for common law conversion, but deny their motion with respect to plaintiff's remaining claims.

## ALLEGATIONS OF FACT[2]

Plaintiff Natalie Brahm is a patient with Hospital Sisters, a hospital system based in Springfield, Illinois. To attract patients, Hospital Sisters encourages individuals to use their website to search for treatments, book appointments, contact providers, and otherwise facilitate their care. Hospital Sisters also hosts a "patient portal," which permits patients to review items like their health records and lab results. Hospital Sisters' privacy policies also make a number of assurances to patients, including that they will not: disclose personal health information ("PHI") without their patients' written authorization; use or disclose sensitive personal information without patients' *express* consent; and directly provide personal identifiable information ("PII") to strategic partners for promotional purposes. Those policies further commit Hospital Sisters to obtain patients' authorization before using PHI for marketing or sales purposes. Finally, nothing in the policies disclose (or seeks consent for) Hospital Sisters' sharing PHI/PII with other companies not involved with the patients' care.

---

and each class member has incurred statutory damages of at least $1,000, as well as uncalculated compensatory and punitive damages, along with attorneys' fees.

[2] In resolving a motion to dismiss under Rule 12(b)(6), the court takes all factual allegations in the complaint not only as true but viewed in a light most favorable to plaintiff, including drawing all reasonable inferences in plaintiff's favor. *Killingsworth v. HSBC Bank Nev.*, 507 F.3d 614, 618 (7th Cir. 2007).

Still, Hospital Sisters has allegedly installed tracking pixels provided by third parties, including Facebook and Google, to collect data about patients' activity on its website and patient portal automatically and without their consent, including conditions for which patients are being treated. Brahm further alleges that she personally visited the Hospital Sisters' website and patient portal several times in 2021, providing personal identifying and health care information, as well as queries related to fertility treatments, which Hospital Sisters then shared with Facebook, Google, and other companies. Worse, according to Brahm, because these tracking pixels installed by Hospital Sisters transfer patient data in real time, advertisers immediately have all the information needed to identify patients and what they did on the website.[3]

## OPINION

Plaintiff asserts six different Wisconsin law claims for conversion, breach of implied contract, wiretapping, breach of confidentiality, invasion of privacy, and unjust enrichment, all of which defendants seek dismissal under Fed. R. Civ. P. 12(b)(6) for failure to state a claim. Accordingly, the court takes up each claim below, beginning with the weakest.

[3] For example, Brahm alleges that "Facebook's Meta Pixel collects and forwards this data to Facebook, including the full referral URL (including the exact subpage of the precise terms being reviewed) and Facebook then correlates the URL with the patient's Facebook user ID, time stamp, browser settings, and even the type of browser used. . . . The captured search terms and the resulting URLs divulge a patient's medical issues, personal interests, queries, and interests on third-party websites operating outside of Facebook's platform." (Dkt. #1-1, at ¶ 166.)

## I. Conversion

Defendants argue that plaintiff's electronic health care records and identifying information are not the proper subject of a conversion claim, which is limited to chattel or identifiable, tangible, and moveable property. *See Md. Staffing Servs., Inc. v. Manpower, Inc.*, 936 F. Supp. 1494, 1507 (E.D. Wis. 1996) (citation omitted) ("Conversion is the wrongful or unauthorized exercise of dominion or control over a chattel."); *see also Epic Sys. Corp. v. Tata Consultancy Servs. Ltd.*, No. 14-cv-748-wmc, 2016 WL 845341, at *27 (W.D. Wis. Mar. 2, 2016) (finding "no support from Wisconsin courts" to include "electronic records that are stored on a computer" as proper subject of conversion claim); *Lands' End, Inc. v. Genesys Software Sys., Inc.*, No. 13-cv-38, 2014 WL 266630, at *3 (W.D. Wis. Jan. 24, 2014) (rejecting claim for conversion of software); *Third Educ. Grp., Inc. v. Phelps*, No. 07-cv-1094, 2009 WL 2150686, at *7 (E.D. Wis. May 15, 2009) (rejecting claims for common law conversion of trademarks, domain name, and corporate name).

While plaintiff does not dispute that her PII/PHI does not qualify as chattel, she argues the Wisconsin Supreme Court held in *Management Computer Services, Inc. v. Hawkins, Ash, Baptie & Co.*, 206 Wis.2d 158, 557 N.W.2d 67 (1996), that a defendant could also be liable for converting *intangible* property. *Id.* at 169, 557 N.W.2d at 72; *see also H.A. Friend & Co. v. Professional Stationery, Inc.*, 2006 WI App 96, ¶ 4, 294 Wis. 2d 754, 720 N.W.2d 96 (allowing conversion claim for "cash on hand and in bank accounts"). Even though *Management Computer Services* involved software, however, the property converted was *physical* software backup tapes taken by an accounting firm's employee and a *printed* copy of the software. *See Danaher Corp. v. Lean Focus, LLC*, No. 19-cv-750-wmc, 2021 WL

3190389, at *19 (W.D. Wis. July 28, 2021) (distinguishing *Management Computer Services* on same ground and granting summary judgment to defendants because a conversion claim does not extend to electronic documents like those at issue in the case); *see also Weather Shield Mfg., Inc. v. Drost*, No. 17-cv-294-jdp, 2018 WL 3824150, at *5 (W.D. Wis. Aug. 10, 2018) (holding misappropriation of intellectual property fails to state claim for conversion under Wisconsin law).[4] Absent a change in Wisconsin law, therefore, plaintiff's claim for conversion will be dismissed.

**II. Breach of Implied Contract**

Plaintiff alleges that defendants breached a promise to confidentially and securely maintain her PII/PHI, which is further protected from disclosure by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and by defendants' fiduciary duty to their patients. Defendants move to dismiss this claim on the grounds that plaintiff: (1) has failed to allege consideration sufficient to form an implied contract under Wisconsin law, *see Scott v. Savers Prop. & Cas. Ins. Co.*, 2003 WI 60, ¶ 45, 262 Wis. 2d 127, 663 N.W.2d 715 ("The general rule is that the performance of a legal duty, or the promise to perform a legal duty, is not sufficient consideration to create a contract."); and (2) alleges damages based on her "overpayment" for medical treatment and underpayment for the interest in her medical records is implausible on its face, *see Dinerstein v. Google, LLC*, 73

[4] In fairness, courts in other states, and the contemporary widespread use of electronic records, have broadened common law conversion claims to include records like those in this case. However, Wisconsin law has yet to support such an expansion, nor will this federal court presume to do so. *See Epic Sys.*, 2016 WL 845341, at *28-29 ("Absent some indication that Wisconsin courts would embrace such an expansion, the court is unwilling to adopt a broader definition of a conversion claim then currently is recognized based solely on intangible property.").

F.4th 502, 516-17 (7th Cir. 2023) (neither overpayment nor underpayment theory of financial harm is plausible where patient alleged hospital disclosed anonymized electronic health records to Google for research purposes). However, neither of defendants' arguments warrants dismissal of plaintiff's breach of implied contract claim at this early stage of the lawsuit.

**A. Consideration**

First, as plaintiff points out, numerous courts have held that promises to keep PII/PHI confidential and private provide sufficient consideration for an implied contract, especially where, as in this case, defendants' privacy policies allegedly include express promises that go well beyond an implicit promise to comply with the law. *E.g.*, *Fox v. Iowa Health System*, 399 F. Supp. 3d 780, 801-802 (W.D. Wis. 2019) (denying motion to dismiss where plaintiffs allege promises that "go beyond state and federal regulations" to payment for "privacy protection as "part of the services" and defendant failed to "provide the full benefit of the bargain"); *Wallace v. Health Quest Sys., Inc.*, 2021 WL 1109727, at *11 (S.D.N.Y. Mar. 23, 2021) (finding adequate consideration because "plaintiffs do not allege defendant promised merely to abide by its legal obligations to protect the Private Information under HIPAA").

For example, plaintiff here alleges that defendants promised, either expressly or implicitly, never to use cookies to retrieve information from patients' computers that are unrelated to defendants' website or provide patients' PII to its strategic partners for promotional purposes, and to implement adequate measures to protect PII/PHI, implement policies and procedures prohibiting the disclosure of patients' PII/PHI without

consent, as well as install adequate firewalls or similar measures to prevent the automatic routing of patients' PII/PHI to third party advertising companies. While defendants point out that plaintiff generally states in her response brief that HIPAA prohibits "the exact same conduct Plaintiff alleges" (dkt. # at 4), the court declines to dismiss a claim for breach of an implied contract on the ground that defendants' express promises of privacy are merely restatements of their preexisting legal obligations under HIPAA or any other statute. Even if this argument had merit, it would depend on factual findings more appropriately considered at summary judgment or trial, not in a motion to dismiss. *See Rudolph v. Hudson's Bay Co.*, No. 18-cv-8472, 2019 WL 2023713, at *11 (S.D.N.Y. May 7, 2019) (declining to dismiss breach of implied contract claim regarding data privacy because "[a]t the pleading stage, the Court is unable to discern the extent to which California's data-protection statute overlaps with any implied promise to maintain data customers' protection").

**B. Damages**

Second, defendants argue that the Seventh Circuit recently rejected overpayment and underpayment theories of financial harm similar to those raised by plaintiff.[5] *Dinerstein,* 73 F.4th at 517. In that case, the court of appeals noted that it had previously "expressed serious skepticism" about an overpayment theory of injury outside the product-liability context, and it was particularly "not inclined to extend [it] to novel contexts" like

[5] The court of appeals explained that Dinerstein's theory of recovery rested on allegations that the medical care he purchased came bundled with a promise of medical confidentiality, and because the defendant failed to deliver on that promise, he allegedly was deprived of the full benefit of his bargain. *Dinerstein*, 73 F.4th at 517.

the breach of medical confidentiality claim at issue in that case. The *Dinerstein* court was "even more skeptical" of plaintiff's underpayment theory seeking to recover any financial benefit defendant received from the unauthorized use of his medical information because: (1) Illinois law does not grant a patient a property interest in his medical records, as they instead belong to the medical provider; and (2) a plaintiff's injury in fact cannot be based *solely* on the defendant's gain, *and* plaintiff had not alleged that defendant's use of plaintiff's medical information somehow deprived him of its economic value. *Id*. at 518.

In response, plaintiff argues that *Dinerstein* is distinguishable on several grounds, citing both federal and Wisconsin court decisions denying motions to dismiss breach of contract and other common law claims seeking similar types of damages in data breach cases. *E.g.*, *Florence v. Ord. Express, Inc.*, 674 F. Supp. 3d 472, 479 (N.D. Ill. 2023) ("Plaintiffs' alleged loss of privacy resulting from the data breach [of social security, driver's license, and tax identification numbers] is a concrete injury in fact."); *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 613 F. Supp. 3d 1284, 1297 (S.D. Cal. 2020) ("The dissemination of one's personal information can satisfy the damages element of a breach of contract claim."); *Doe 1 v. AOL LLC*, 719 F. Supp. 2d 1102, 1111 (N.D. Cal. 2010) (California Consumers Legal Remedies Act claim in which plaintiffs sufficiently alleged they did not receive benefit of bargain where internet service company collected and disclosed "undeniably sensitive information"); *Bray v. Gamestop Corp.*, No. 17-cv-1365, 2018 WL 11226516, at *4 (D. Del. Mar. 16, 2018) ("[P]laintiffs have plausibly alleged that data security was part of what they paid for but did not receive."); *Ostrenga Excavating, Inc. v. Cleveland Constr., Inc.*, 2017 WI App 80, ¶ 65, 378 Wis. 2d 739, 905 N.W.2d 84

(holding with respect to implied contract claim in contract case that "when a breaching party partially performs, the nonbreaching party is entitled to the value of the performance promised minus the value of what the breaching party actually rendered."); *W.H. Fuller Co. v. Seater*, 226 Wis. 2d 381, 385-86, 595 N.W.2d 96, 99 (Ct. App. 1999) (explaining that appropriate measure of damages for contract implied in fact is based on quantum meruit, which is measured by reasonable value of plaintiff's services).

While defendants contend that the cases cited by plaintiff all involve different types of claims and damages than those sought in this case, plaintiff argues that *Dinerstein* does not necessarily present an absolute bar to damages in her case. The court agrees, at least at this early stage in the lawsuit.

*First*, the court in *Dinerstein*, 73 F.4th at 514-15, found that plaintiff's alleged damages were too speculative because the disclosed patient records were *anonymized*, and plaintiff failed to allege that any *specific identifying information* had evaded redaction. Nor was it alleged that Google had taken any steps to identify the plaintiff or intended to identify the plaintiff in the future. In contrast, plaintiff alleges here that the personal medical information disclosed to Facebook and other third-party sites was *not anonymized*. Further, although defendants argue that plaintiff has not named any third party other than Facebook having her actual identity or being able to link her PII/PHI to her identity, the allegations as to Facebook are certainly enough to get past the preliminary stage. Moreover, plaintiff has also sufficiently alleged that other advertisers not only designed various ways to gain access to identifying information for Hospital Sisters' patients, but had all the information needed to identify patients and what they did on defendants'

websites. Whether this is true, and whether plaintiff voluntarily disclosed her PII/PHI to Facebook or gave her consent to receive targeted advertising from other third-party advertisers, are issues best resolved on summary judgment or at trial.

*Second*, unlike in *Dinerstein*, plaintiff does not appear to base her damages solely on defendants' gain. Rather, she specifically alleges that defendants' unauthorized disclosures "diminished the sales value" of her PHI (dkt. #1-1, at ¶ 283), which is the very allegation found lacking in the complaint in *Dinerstein*. Regardless, plaintiff also alleges that she continues to suffer compensable injuries resulting from the release and disclosure of her PII/PHI. *See Yockey v. Salesforce, Inc.*, 2023 WL 5519323, at *3 (N.D. Cal. Aug. 25, 2023) (Plaintiffs' allegations that Salesforce collected personal health information during website chat communications "give rise to a concrete injury [under state privacy statute]" because Salesforce "necessarily deprived Plaintiffs of their control of their information."). Of course, further development of the record may show that plaintiff's damages theories are no more plausible than those rejected by the Seventh Circuit in *Dinerstein* (or other district courts in some of the cases cited by defendants),[6] but in light of the more robust affirmative

[6] *E.g.*, *B.K. v. Eisenhower Med. Ctr.*, 2024 WL 878100, at *7 (C.D. Cal. Feb. 29, 2024) (holding plaintiffs did not persuasively allege reasonable expectation of compensation for value of their personal information, or that they were foreclosed from capitalizing on value of their personal information); *In re Practicefirst Data Breach Litig.*, No. 21-cv-790, 2022 WL 354544, at *7 (W.D.N.Y. Feb. 2, 2022), *rep. and rec. adopted*, 2022 WL 3045319 (W.D.N.Y. Aug. 1, 2022) ("[P]laintiffs do not allege that they attempted to sell their personal information and were forced to accept a decreased price, nor do they allege any details as to how their specific, personal information has been devalued because of the breach."); *In re SuperValu, Inc., Customer Data Sec. Breach Litig.*, No. 14-md-2586, 2018 WL 1189327, at *16 (D. Minn. Mar. 7, 2018) (finding defendant did not obtain any unjust benefit because plaintiff "does not allege that the goods he purchased were defective or that their value was somehow diminished by the data breach").

allegations of injury, the court will not dismiss plaintiff's breach of implied contract claim on this ground without room to develop the record.

**III. Wiretapping**

Plaintiff asserts a claim under the Wisconsin Wiretap Act, Wis. Stat. § 968.31(1), which prohibits the interception and disclosure of electronic communications, defined as "any transfer of . . . data or intelligence of any nature wholly or partially transmitted by a wire, radio, electromagnetic, photoelectronic or photooptical system." Wis. Stat. § 968.27. Plaintiff alleges that defendants here violated the statute by embedding tools on their seemingly private and confidential websites, automatically rerouting patients' PII/PHI to others for their unauthorized use.[7] While defendants argue that they are exempt from liability as a party these alleged confidential communications, *see* Wis. Stat. § 968.31(2)(c), that exemption may not apply if "the communication is intercepted for the purpose of committing any criminal or tortious act in violation of the constitution or laws of the United States or of any state or for the purpose of committing any other injurious act," *id*. At least in the context of the federal wiretap statute, 18 U.S.C. § 2511(2)(d), courts apply a similar "crime-tort exception" only "where the defendant allegedly committed a tortious or criminal act independent from the act of recording itself." *Kurowski v. Rush Sys. for Health (Kurowski II)*, No 22-cv-5380, 2023 WL 4707184, at *4 (N.D. Ill. July 24, 2023) (internal citations omitted); *see also Okash v. Essentia Health*, No. 23-cv-482, 2024 WL 1285779, at *4 (D. Minn. Mar. 26, 2024) (citing *Kurowski* and further explaining that the qualifying

[7] Subsection 968.31(2)(m) allows any person whose communication is intercepted or disclosed to bring a civil action against the wiretapper.

bad acts must be "secondary to the acquisition of the communication" and involve "tortious or criminal use of the interception's fruits").

In this case, plaintiff alleges that defendants intercepted patients' electronic communications *for the purposes* of making disclosures that violated HIPAA, 42 U.S.C. § 1320d-6(a)(3) (criminal wrongful disclosure of individually identifiable health information), as well as state tort law, then bartered away patients' PII/PHI to third parties like Facebook and Google for marketing and advertising benefits. While defendants argue that marketing and advertising are not criminal or tortious acts, plaintiff plausibly alleges that defendants committed a criminal or tortious act by *disclosing* -- versus merely *intercepting* -- patients' PII/PHI.

Defendants further argue that federal courts have refused to apply the crime-tort exception when, as here, a plaintiff's affirmative allegations establish that defendants' primary motivation in intercepting the communications was making money, *not* injuring plaintiff. *E.g.*, *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 797 (N.D. Cal. 2022) (noting in context of injunction that "[m]ultiple courts in this district have found that the crime-tort exception to the Wiretap Act is inapplicable where the defendant's primary motivation was to make money"); *Desnick v. Am. Broad. Companies, Inc.*, 44 F.3d 1345, 1353 (7th Cir. 1995) (dismissing state and federal wiretap claims because no suggestion that defendants ordered ophthalmic test patients with concealed cameras to commit a crime or tort, even though eventual television broadcast of clinic footage was tortious). However, defendants have not cited definitive support for this proposition by the Seventh Circuit or this district, unlike decisions in the Ninth Circuit and the Northern District of California,

finding the crime-tort exception to the Wiretap Act inapplicable in *all* cases in which the defendant's primary motivation was to make money. *See In re Grp. Health Plan Litig.*, No. 23-cv-267, 2023 WL 8850243, at *8 (D. Minn. Dec. 21, 2023) (finding same).

Defendants also cite the Northern District of Illinois's holding in *Kurowski II* and the Wisconsin Court of Appeals' decision in *Bach v. Kopatich*, 2012 WI App 11, ¶ 16, 338 Wis. 2d 486, 808 N.W.2d 742, as additional support for their argument, but both cases are distinguishable and do not support a blanket limitation under the crime-tort exception advocated by defendants. In *Kurowski II*, the district court dismissed plaintiff's federal wiretap claim on the ground that his allegations were "far too vague to allow an inference to be drawn that [defendant] was actually disclosing [specific health information] as it is unambiguously defined by HIPAA, rather than just metadata." 683 F. Supp. 3d at 843. Indeed, after Kurowski amended her complaint to more specifically identify and describe the information transmitted to third parties for defendant's alleged financial gain, the court found her allegations sufficient to "invoke the HIPAA exception-to-the-party-exception" and state a wiretap claim. *Kurowski v. Rush Sys. for Health* (*Kurowski III*), No. 22-cv-5380, 2023 WL 8544084, at *3 (N.D. Ill. Dec. 11, 2023). Similarly, in *Bach*, the Wisconsin Court of Appeals dismissed a plaintiff's state wiretap claim because he failed to offer evidence that the taping at issue "was done for the purpose of attempting to have him disciplined or discharged" at summary judgment, did "not deny using the vulgar, derogatory language . . . of which he is accused," and failed to show that "[f]iling a harassment complaint or providing evidence of [his] admitted misconduct to an employer" was unlawful. 2012 WI App 11, ¶ 16.

At this early stage, therefore, the court finds that plaintiff has plausibly alleged that defendants' primary motivation in intercepting and disclosing patients' PII/PHI was to commit wrongful and tortious acts -- namely, the disclosure and use of patient data for advertising, marketing, and revenue generation without their express written consent. *See In re Grp. Health Plan Litig.*, 2023 WL 8850243, at *8 (concluding same in denying motion to dismiss federal wiretap claim). Moreover, the parties' arguments about whether the crime-tort exception can be invoked in this case, and whether applying the exception would create an absurd result for Wisconsin Wiretap Law, are more appropriately addressed at summary judgment after the record has been more fully developed.

**IV. Breach of Confidentiality**

To state a claim for breach of fiduciary duty under Wisconsin law, plaintiff must plausibly allege that: (1) defendants owed her a fiduciary duty; (2) defendants breached that duty; and (3) the breach caused plaintiff damage. *Berner Cheese Corp. v. Krug*, 2008 WI 95, ¶ 40, 312 Wis.2d 251, 270, 752 N.W.2d 800; *see also Jackson v. McKay-Davis Funeral Home, Inc.*, 830 F. Supp. 2d 635, 648 (E.D. Wis. 2011) (citing same). As to the first element, whether a fiduciary duty is owed is a question of law. *Zastrow v. Journal Communications, Inc.*, 2006 WI 72, ¶ 12, 291 Wis.2d 426, 437, 718 N.W.2d 51. A fiduciary is one who accepts a "position of authority with regard to the affairs of another," *id*. ¶ 25, and "fiduciary duty" describes "those obligations that are peculiar to a fiduciary and are based on the conscious undertaking of a special position with regard to another," *id*. ¶ 28. Whether created by contract or formal legal relationship or implied in law from the factual situation surrounding the parties' transactions and relationships, "[m]anifest in the

existence of a fiduciary relationship is . . . an inequality, dependence, weakness of age, of mental strength, business intelligence, knowledge of facts involved, or other conditions giving to one an advantage over the other." *Prod. Credit Ass'n of Lancaster v. Croft*, 143 Wis. 2d 746, 755, 423 N.W.2d 544, 547 (Ct. App. 1988).

In arguing that Wisconsin law does not recognize a healthcare provider's fiduciary duty to maintain a patient's confidentiality, defendants rely on two cases that do not even involve the disclosure of a patient's health care information. *See Linman v. Marten Transp., Ltd.*, No. 22-cv-204, 2023 WL 2562712, at *7 (W.D. Wis. Mar. 17, 2023) (finding job applicant failed to state independent claim for breach of confidence against potential employer for personal information lost during a data breach); *Rock Hill Dairy, LLC v. Genex Coop., Inc.*, 2020 WL 7042837, at *6 (W.D. Wis. Dec. 1, 2020) (finding plaintiff's allegations regarding non-payment for sale of bulls suggested "nothing greater than the typical expectations held by parties to a contract"). Moreover, as plaintiff points out, "[s]ome federal courts applying Wisconsin law have stated that the concept of 'breach of confidentiality' is relevant to . . . professional negligence claims where the defendant owed the plaintiff a duty of confidentiality." *Linman*, 2023 WL 2562712, at *7 (citing *Smith v. Dep't of Corr. of State of WI*, 2005 WL 2449841, at *24 (E.D. Wis. Sept. 30, 2005)). Indeed, in *Steinberg v. Jensen*, 194 Wis. 2d 439, 465-66 (1995), the Wisconsin Supreme Court specifically held that "[p]hysicians owe an ethical duty of confidentiality to their patients," and "[t]his ethical duty generally prohibits a patient's treating physicians from disclosing confidential information without the patient's consent." Finally, Wis. Stat.

§ 146.81 provides that patient health care records may be released only with the informed consent or authorization of the patient, or to persons otherwise designated by the statute.

Accordingly, the court concludes that plaintiff has plausibly alleged both a fiduciary duty and a breach of that by defendants in failing to maintain the confidentiality of their patients' health care records. As for defendants' additional arguments as to the third element, the court has already held that plaintiff plausibly alleges causation -- despite her giving Facebook permission to gather information from third-party websites, including by signing up as a Facebook user -- and resulting damages. Similarly, the court has explained why causal damages questions are better addressed on a fuller record than offered on the pleadings alone.

**V. Invasion of Privacy**

Plaintiff initially alleged that defendants invaded her right to privacy as defined by Wis. Stat. § 995.50(2), both by intrusion into and the public disclosure of her private identifying health information, but she is now willing to dismiss any claim of "intrusion." To state a publication of private information claim, plaintiff must plausibly allege: (1) a "public disclosure;" (2) of "private facts;" (3) on a matter that is "highly offensive to a reasonable person of ordinary sensibilities;" and (4) that defendants acted "unreasonably or recklessly" when disclosing plaintiff's information. *Pachowitz v. Ledoux*, 2003 WI App 120, ¶ 18, 265 Wis. 2d 631, 666 N.W.2d 88 (internal citation omitted). In their motion to dismiss, defendants argue that plaintiff fails to satisfy the first and third requirements. As to the first, they again point out the alleged disclosure of PII/PHI was made only to one *named* entity and not to the public at large. *See Nabozny v. Optio Sols., LLC*, 583 F. Supp.

3d 1209, 1213 (W.D. Wis. 2022) ("Publicity goes beyond sharing with one person; the communication must be 'to the public at large,' or to enough people that the information is certain to become public knowledge."). As to the third, defendants contend that the information disclosed did not involve a matter "highly offensive to a reasonable person." *See Mosley v. Oakwood Lutheran Senior Ministries*, 2023 WL 4782874, ¶ 32 (Wis. Ct. App. July 27, 2023) (finding "no authority in which the disclosure of a positive COVID-19 test result, or other analogous information, was deemed highly offensive to a reasonable person of ordinary sensibilities").

Since the complaint at least alleges defendants granted access to a wider group of companies and disclosure of private health information that may well include matters that a reasonable person of ordinary sensibility would find highly offensive, both arguments are more appropriately addressed on summary judgment or at trial. For now, plaintiff's allegations that defendants transferred information related to her infertility issues, which she alleges is associated with societal stigma and personal anguish, to various technology companies that employ hundreds of thousands of employees who have access to this information, are deemed sufficient to state at least a plausible claim for invasion of privacy.

**VI. Unjust Enrichment**

Finally, as an alternative to her breach of implied contract claim, plaintiff asserts a claim for unjust enrichment, which requires the following three elements: (1) a benefit conferred by plaintiff to defendants; (2) defendants' knowledge of the benefit; and (3) defendants' retention of the benefit under circumstances making it inequitable without payment of the benefit's value. *Admiral Ins. Co. v. Paper Converting Mach. Co.*, 2012 WI 30,

339 Wis. 2d 291, 811 N.W.2d 351. Here, as previously discussed, plaintiff alleges that she conferred two types of benefits on defendants: (1) payment for health care services that included defendants' obligation to protect her PHI/PII, which defendants failed to provide; and (2) valuable and sensitive medical information that defendants captured and monetized through advertising, sales, or trade for other services.

While defendants again contend that plaintiff's overpayment and underpayment theories of benefits conferred on defendants are implausible, that argument fails for reasons already addressed in conjunction with plaintiff's breach of implied contract claim. *See Fox*, 399 F. Supp. 3d at 802-03 (denying motion to dismiss unjust enrichment claim related to hack of health services network's email system where plaintiff alleged defendants failed to provide her with the privacy protection she paid for as *part* of her health care services). All of defendants' remaining contentions -- that plaintiff did not allocate any of her health care services payments to defendants for data privacy, paid more for health care than patients who did not access defendants' websites, voluntarily disclosed her PII/PHI to Facebook, and gave her consent to receive "targeted advertising" -- are contrary to the factual allegations in the complaint or reasonable inferences from those facts, both of which this court must accept at the pleading stage.

While further development of the record may prove that many, if not all, of defendants' factual contentions are true beyond reasonable dispute, plaintiff's allegations are sufficient at this early stage to state a legal claim for unjust enrichment. Of course, defendants may challenge these allegations and renew their arguments with respect to this

(and any of plaintiff's other remaining claims) at summary judgment, but their present motion is premature.

ORDER

IT IS ORDERED that defendants' motion to dismiss (dkt. #16) is GRANTED IN PART and DENIED IN PART as follows:

1) The motion to dismiss plaintiff Brahm's claim for conversion is GRANTED; and

2) Defendants' motion is DENIED in all other respects.

Entered this 28th day of June, 2024.

BY THE COURT:

/s/

_____

WILLIAM M. CONLEY
District Judge