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

NATALIE BRAHM, JAMES QUAID,
SUE BORNEMANN, and KIM WARD,
on behalf of themselves and
similarly-situated individuals,

Plaintiffs,

v.

HOSPITAL SISTERS HEALTH SYSTEM,
SACRED HEART HOSPITAL OF THE HOSPITAL
SISTERS OF THE THIRD ORDER OF ST. FRANCIS,
PREVEA HEALTH SERVICES, INC., and
PREVEA HEALTH NETWORK, INC.,

Defendants.

OPINION and ORDER

23-cv-444-wmc

Defendants removed this lawsuit to federal court by invoking the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d).[1] Plaintiffs Natalie Brahm, James Quaid, Sue Bornemann, and Kim Ward assert that the defendants installed digital marketing and automatic rerouting tools on their websites that routinely disclose their patients' identities and protected health care information to third-party websites like Google without the patients' knowledge or consent in violation of federal and state wiretapping statutes,[2] as well as Wisconsin common and

[1] Plaintiff Brahm originally filed this lawsuit in the Eau Claire County Circuit Court on April 24, 2023, against defendants Hospital Sisters Health Systems and Sacred Heart Hospital of the Hospital Sisters of the Third Order of St. Francis (collectively "HSHS"), who then removed to this federal court and moved to dismiss for failure to state a claim. (Dkt. ##1-1 and 16.) In denying defendants' motion (except as to Brahm's Wisconsin common law claim for conversion, which was dismissed), this court found the jurisdictional requirements of CAFA were met based on defendants' representations in their notice of removal. (Dkt. #42, at 1 n.1.) After discovery commenced, the court granted the parties' joint motion for leave to amend Brahm's original complaint to add three new plaintiffs, add Prevea Health Services, Inc. and Prevea Health Network, Inc. (collectively "Prevea") as defendants, assert new claims, and propose subclasses. (Dkt. #50.)

[2] Specifically, plaintiffs assert claims under the Federal Wiretap Act, the Wisconsin Wiretapping Act, and the Illinois Eavesdropping Statute. (Dkt. #51, at 62, 69, and 78.)

statutory laws for breach of duty of confidentiality, breach of implied contract to protect privacy, public disclosure of private facts, and unjust enrichment. (*See* Amd. Cpt., dkt. #51.)

Four motions raising overlapping issues are pending before the court: plaintiffs move to (1) certify four, related subclasses under Rule 23 of the Federal Rules of Civil Procedure with respect to their claims under federal and Wisconsin state law (dkt. ##68, 90),[3] and (2) strike the report and testimony of defendants' technical expert, James Vint (dkt. #120); while defendants move (3) to strike the expert report and testimony of plaintiffs' damages expert, Eric Krause (dkt. #129), and (4) for summary judgment as to all of plaintiffs' claims (dkt. #131). For reasons explained more fully below, the court finds that plaintiffs have failed to present sufficient evidence of a concrete and particularized injury-in-fact, actual or imminent, and traceable to the defendants' conduct, depriving them of Article III standing to pursue any of their claims in federal court. Accordingly, the court will remand the lawsuit for lack of subject matter jurisdiction to state court and deny the parties' remaining motions as moot.

UNDISPUTED FACTS[4]

A. Background

Plaintiffs are all patients of one or more of the defendants. Defendant HSHS is a regional health system that operates hospitals and clinics throughout Wisconsin and Illinois;

---

[3] In their brief in support of their motion for class certification, plaintiffs represent that, for reasons of simplicity, they are "not moving to certify classes asserting claims under Illinois law, including the Illinois wiretapping claim." (Dkt. #68, at 26 n.4.)

[4] Unless otherwise indicated, the following facts are deemed material and undisputed for purposes of summary judgment. The court has drawn these facts from the parties' proposed findings of fact and responses, as well as from the record evidence as appropriate, when considered in the light most favorable to plaintiffs as the non-moving party. *McGee v. Parsano*, 55 F.4th 563, 566 (7th Cir. 2022).

and defendant Prevea is a healthcare organization based in Wisconsin that provides primary and specialty health care in clinic and hospital settings in more than 70 locations across northern and eastern portions of Wisconsin.

Defendants operate public websites and authenticated MyChart portals as MyHSHS and MyPrevea, respectively, which allow patients to log in with a username and password to access their medical records, schedule appointments, and pay bills. The portals also allow for proxy access, meaning that family members, legal representatives, or another authorized individual can use the portal on a patient's behalf. While both portals are regularly accessed through web browsers, MyPrevea is available as an iOS and Android mobile application. In addition, MyHSHS and MyPrevea share user data, so patients seen by both healthcare organizations may log into MyPrevea and also see their medical records from HSHS or log into MyHSHS and see their Prevea medical records.

At least two of the four named plaintiffs have used one or both of defendants' patient portals at various times within the proposed class periods.[5] Plus, they all use Facebook on a near-daily basis and have Google accounts, the latter of which were created by providing Google with various pieces of their personal information, including names, dates of birth, and physical addresses. While plaintiffs began seeing Facebook advertisements related to their specific medical conditions after visiting defendants' portals or websites, all four also searched or posted about their medical conditions or treatment online and have had their personal information involuntarily exposed to third parties by entities other than defendants.

---

[5] The parties dispute whether named plaintiffs James Quaid and Kim Ward used defendants' portals within the relevant periods for the putative class.

B. Defendants' Privacy Policies

As required by federal and state law, defendants have privacy policies promising never to disclose a patient's protected health information (referred to as "PHI") for advertising or marketing purposes without that patient's permission.[6] To this end, defendants developed a "deidentification" policy that defines PHI in the same way that "individually identifiable information" is defined under HIPAA, which includes any information that (1) is created by or received by defendants; (2) identifies an individual; or (3) provides a "reasonable basis to believe the information can be used to identify an individual," and relates to a person's "past, present or future physical or mental health." (Dkt. #70-2; 42 U.S.C. § 1320d.) Defendants' policy further defines "disclosure" as the "release, transfer, provision of access to, or divulging in any other manner, of information outside the organization." (*Id.*)

Defendants' privacy policies also contain specific guidelines for redacting 19 different patient identifiers, including a person's name, address, and digital identifiers associated with their devices (such as internet protocol ("IP") address numbers, Uniform Resource Locators ("URLs"), and any other unique identifying number, characteristic, or code). These "de-identification" policies similarly derive from and cite HIPAA Privacy Rule, 45 CFR § 164.514, which requires providers to exclude any identifiers when disclosing patient data to third parties without the patient's consent.

[6] At all times relevant to plaintiffs' claims, both HSHS and Prevea relied on third-party vendors to manage the advertising technology on their websites.

C. Defendants' Use of Google Analytics

Between at least 2016 and 2023, defendants deployed Google Analytics tracking technology on their public websites, within patient portals on their websites, and on MyPrevea's login page and Android app. Specifically, whenever a user visits defendants' websites or portals, Google Analytics gathers information about the user's interactions and shares certain transmissions with Google. Among other things, the parties dispute: who made the decision to install the technology; the reasons they installed it; what defendants knew about Google Analytics and the information it collected; when defendants gained any such knowledge; how Google Analytics worked on defendants' websites and portals; what information it disclosed (if any) about website or portal visitors; and whether the data transmitted by Google Analytics was capable of identifying a particular individual, or ever actually identified any individual.

In further support of their contradictory views, plaintiffs have submitted the expert reports of Dr. Zubair Shafiq, a Professor of Computer Science at the University of California-Davis whose research focuses on online privacy, security, and safety; while defendants have submitted the expert reports of Mr. James Vint, Managing Director at Secretariat Advisors, LLC, an international consulting firm specializing in expert services related to data privacy.[7]

[7] Because Vint did *not* test defendants' websites or even the same version of the tracking technology defendants deployed, plaintiffs have moved to strike Vint's expert opinions as unreliable, irrelevant, and unduly confusing under Fed. Rs. Evid. 403 and 702, and *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), noting that even Vint concedes that the appropriate methodology for testing technology on a website is to investigate the website itself "as it is" or to recreate it "as it was" using archived materials. (Dkt. ##120, 122 at 94-97.) While the court finds some merit in these arguments, it is unnecessary to consider Vint's reports, because as discussed below, Dr. Shafiq's expert opinions fail to provide sufficient evidence to support plaintiffs' standing. Therefore, the court will deny plaintiffs' motion to strike as moot without recounting Vint's contrary opinion here.

For his part, Dr. Shafiq explains the following with respect to how data is collected by Google Analytics:

- Defendants' patient's web browser or app sends a series of requests using the Hypertext Transfer Protocol ("HTTP") protocol to upload files from or download files to a website's server.

- An HTTP request contains an IP address, which is an identifier assigned to any internet-connected device, and an URL, which represents the address of the file that a web browser is requesting from a web server.

- Among other things, a full-string page URL contains: the server's domain name; the path of the file located on the server that is being requested; and a list of query parameters that contain additional information being sent from a web browser to a web server.

- By collecting two types of data in HTTP requests from a user's web browser -- the identifiers and browsing activity -- tracking technologies such as Google Analytics and Firebase Analytics[8] allow a third party to tell, among other things, that a user visited website A at time A, website B at time B, and so on. The identifiers stored in cookies include an account identifier, which is akin to a person's driver license number, and a device identifier, which is akin to the vehicle's license plate number. Browsing activity is collected via the URL, referrer header (or URL of the previous webpage from which the current webpage was followed), or payload (containing more detailed information, such as a description of a product or service shown on the webpage).

- Google Analytics works by adding a small piece of code to each page on a website, which is triggered whenever someone loads a page. Thus, when defendants' patients logged into and navigated their portal (e.g., scheduling appointments, viewing test results, and paying bills), defendants shared the patient's IP addresses, user agent data, browser fingerprints, and Google cookies with Google. Some of the information collected by Google Analytics contain full-string, detailed URLs with terms such as "Schedule an Appointment," "Test Results," . . . and "Billing Account Summary."

(Dkt. #88, at ¶¶ 15-20, 27-28, 30, 33, 37-38, 51-59.)

[8] This technology is used on mobile apps.

D. Proposed Class Claims

Plaintiffs have moved to certify four, separate subclasses covering distinct, but overlapping time periods between 2016 and 2023: (1) HSHS patients who accessed the MyHSHS portal through a web browser; plus three classes of Prevea patients who accessed the MyPrevea portal through (2) a web browser, (3) a mobile app, or (4) a link within a text message or email notification. While plaintiffs assert their federal and Wisconsin-state wiretapping claims and Wisconsin common law claims for breach of implied contract, breach of confidentiality, and invasion of privacy on a class-wide basis, they make clear that they are not asserting class claims for unjust enrichment, violations of the Illinois Eavesdropping statute, or defendants' alleged disclosure of private health information to Facebook (as opposed to Google). (*See* dkt. #68, at 1, 26 n.4, and 30-35.)

None of the named plaintiffs have ever tried or intended to sell their personal health information, nor do they claim to have suffered any out-of-pocket expenses as a result of defendants' allegedly wrongful disclosures. Nonetheless, they seek actual damages based on the alleged "diminished sales value of their PHI," as well as statutory and nominal damages. In support, Eric Krause, a director at Applied Economics Consulting Group, Inc. in Austin, Texas, has submitted an expert opinion on behalf of plaintiffs that purports to estimate the fair market value of plaintiffs' confidential data at $175 per person, which he calculated by comparing what a person would pay to maintain the data in confidence with what they would accept to disclose it.[9]

[9] Citing Rule 702 and *Daubert*, defendants have moved to exclude Krause's opinion on the grounds that it is not based on any identifiable calculation or methodology and purports to establish the fair market value of data that plaintiffs would never sell. (Dkt. #129.)

OPINION

Plaintiffs assert various Wisconsin common law and statutory claims related to the confidentiality and privacy of their personal health information, as well as federal and Wisconsin state wiretapping claims.[10] Defendants have moved for summary judgment, arguing that even considering Dr. Shafiq's expert opinions and the other evidence of record in a light most favorable to plaintiffs, a reasonable jury could not find: (1) the injury and causation elements of plaintiffs' claims for breach of implied contract, breach of confidentiality, invasion of privacy, and unjust enrichment; or (2) the interception, party, and content elements of their wiretapping claims. *See* Fed. R. Civ. P. 56(a) (Summary judgment is appropriate if the moving party demonstrates that "there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law."); *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 252 (1986) (If the moving party meets this burden, the non-moving party must provide evidence, which viewed in a light most favorable to it, permits the jury to reasonably find for the nonmoving party.).

While defendant's summary judgment motion fails to address the issue directly, defendants' arguments call plaintiffs' standing into question, as plaintiffs themselves recognize and discuss in their response brief. Moreover, even though this court allowed the original named plaintiff, Brahm, to proceed past the motion to dismiss stage because it found her allegations of injury sufficient at the pleading stage, *Brahm v. Hosp. Sisters Health Sys.*, No. 23-cv-444-wmc, 2024 WL 3226135, at *4 (W.D. Wis. June 28, 2024), standing is a "threshold

[10] Despite HSHS's operations in Wisconsin and Illinois, the parties agree for purposes of summary judgment that Wisconsin law applies to all of plaintiffs' common law claims. In addition, because plaintiffs state that they "do not contest dismissing their Illinois Eavesdropping [claim] given their focus on federal and Wisconsin-based claims" (dkt. #157, at 32 n.14), the court need not address those claims.

question" that "is jurisdictional and cannot be waived." *Dinerstein v. Google, LLC*, 73 F.4th 502, 511 (7th Cir. 2023) (citing *Nettles v. Midland Funding LLC*, 983 F.3d 896, 899 (7th Cir. 2020)). Thus, not only does the court have a duty to ensure that standing is "secured at each stage of the litigation," but "[o]nce the allegations supporting standing are questioned as a factual matter -- either by a party or by the court -- [plaintiffs must make] a showing by a preponderance of the evidence, or proof to a reasonable probability, that standing exists." *Bazile v. Fin. Sys. of Green Bay, Inc.*, 983 F.3d 274, 278 (7th Cir. 2020) (citing *McNutt v. Gen. Motors Acceptance Corp. of Ind.*, 298 U.S. 178, 189 (1936); *Retired Chi. Police Ass'n v. City of Chicago*, 76 F.3d 856, 862 (7th Cir. 1996)); *see also Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 412 (2013) (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992)) ("[A]t the summary judgment stage, [plaintiffs] 'can no longer rest on . . . mere allegations, but must set forth by affidavit or other evidence specific facts."')). With the benefit of a full record at summary judgment, even considering Dr. Shafiq's expert opinions and the other evidence of record in a light most favorable to plaintiffs, the court finds that plaintiffs lack standing to bring any of their claims in federal court.

I. Standing Doctrine

Article III of the Constitution limits the jurisdiction of the federal courts to "cases and controversies" to ensure that the judiciary "confines itself to its constitutionally limited role of adjudicating actual and concrete disputes, the resolutions of which have direct consequences on the parties involved." *Pierre v. Midland Credit Mgmt., Inc.*, 29 F.4th 934, 937 (7th Cir. 2022) (quoting *Genesis Healthcare Corp. v. Symczyk*, 569 U.S. 66, 71 (2013)). To have standing in federal court, a plaintiff must have suffered: (1) a concrete and particularized injury-in-fact;

(2) that is traceable to the defendant's conduct; and (3) that can be redressed by judicial relief. *Id.* at 937 (citing *Lujan*, 504 U.S. at 561 (1992)). To remain in federal court at summary judgment, therefore, evidence must be offered demonstrating that plaintiffs (including the named plaintiffs and every putative class member) satisfy these elements "in the face of any adverse evidence introduced." *Id.* at 939; *see also TransUnion LLC v. Ramirez*, 594 U.S. 413, 431 (2021) ("Every class member must have Article III standing in order to recover individual damages. . . [and] must maintain their personal interest in the dispute at all stages of litigation."). Moreover, "standing is not dispensed in gross; rather, plaintiffs must demonstrate standing for each claim that they press and for each form of relief that they seek." *TransUnion*, 594 U.S. at 431.

Here, plaintiffs' standing hinges on the injury-in-fact element, and more specifically, the concreteness, imminence, and causation requirements. The Seventh Circuit has found concrete harms to include "traditional tangible harms, such as physical harms and monetary harms, as well as [v]arious intangible harms, such as reputational harms, disclosure of private information, and intrusion upon seclusion." *Pierre*, 29 F.4th at 938 (internal quotations and citations omitted). "While the concreteness requirement examines the substance of a plaintiff's asserted injury, the imminence requirement measures its likelihood. In other words, to provide a basis to sue in federal court, an injury must exist in both a qualitative and a temporal sense." *Dinerstein*, 73 F.4th at 511 (internal citation omitted). The Supreme Court has described a concrete injury as one that is real and not abstract, whereas imminent means the injury is not too speculative. *Id*. at 511-12 (citing *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340 (2016); *Lujan*, 504 U.S. at 564 and n.2). In other words, "a plaintiff who has not suffered a past harm cannot simply rest on allegations that he may suffer some possible future injury at some indefinite

future time," and "while an imminent risk of future harm may suffice to support standing to sue for prospective relief (i.e., an injunction), a claim for damages requires a concrete harm that has in fact occurred." *Id.* at 512 (internal citations omitted). With these fundamental principles of standing in mind, the court turns to plaintiffs' claims in this case.

II. Plaintiffs' Claims

Plaintiffs base all six remaining causes of action in their amended complaint on their claim that defendants worked together to install Google Analytics on the HSHS and Prevea patient portals, which allegedly resulted in the disclosure of their patients' identities and health data to Google and Facebook. Plaintiffs further contend that defendants had a duty to maintain patient confidentiality, as HIPAA and their own privacy policies mandate, regardless of what plaintiffs or other third parties may have disclosed with respect to their PHI. Thus, even if plaintiffs *choose* to share their health conditions with their own family members, that does not give *defendants* permission to discuss it with their families or anyone else. For relief, they seek actual damages based on the alleged "diminished sales value of their PHI," as well as statutory and nominal damages.[11] To streamline its discussion, the court begins with plaintiff's tort claims for invasion of privacy and breach of fiduciary duty because the asserted injury underlying these claims is common to plaintiffs' claims for breach of implied contract, unjust enrichment, and violations of wiretapping statutes.

[11] Although plaintiffs do not request injunctive relief expressly, they do assert in their amended complaint that "[u]nless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to inflict irreparable injury to Plaintiffs." (Dkt. #51, at ¶ 331.)

A. Tort Claims

Plaintiffs' claim for invasion of privacy is based on the public disclosure of private facts under Wis. Stat. § 995.50(2)(am)(3), which is one of four types of invasion of privacy actions recognized in Wisconsin. To prevail and be entitled to compensatory damages, equitable relief, and attorney fees under § 995.50(1), plaintiffs must prove: (1) a public disclosure of facts regarding each plaintiff; (2) the facts disclosed are private facts; (3) the private matter made public is one which would be highly offensive to reasonable person of ordinary sensibilities; and (4) defendants intended the disclosure. *Reetz v. Advoc. Aurora Health, Inc.*, 2022 WI App 59, ¶¶ 18 and 20, 405 Wis. 2d 298, 983 N.W.2d 669 (internal citations omitted). Further, for their related claim for breach of fiduciary duty, plaintiffs must prove that: (1) defendants owed them a duty; (2) defendants breached that duty by disclosing plaintiffs' PHI to third parties without their authorization or consent; and (3) the breach caused plaintiff's damage. *Berner Cheese Corp. v. Krug*, 2008 WI 95, ¶ 40, 312 Wis. 2d 251, 752 N.W.2d 800. Here, plaintiffs base their breach of fiduciary duty claim on the "ethical duty of confidentiality" owed to patients, as recognized by the Wisconsin Supreme Court in *Steinberg v. Jensen*, 194 Wis. 2d 439, 465, 534 N.W.2d 361 (1995). (Dkt. #51, at ¶¶ 314-18.)

As evidence for the common element of disclosure under these tort claims, plaintiffs rely solely on Dr. Shafiq's expert opinion that defendants shared certain "identifiers"[12] and

[12] These identifiers included IP address, user agent, and device properties, along with cookies in the case of website logins, and app instance and advertising identifiers in the case of MyPrevea's Android app. (Dkt. #88, ¶¶ 14(a) and (d).)

health-related content information[13] with Google, which is then *capable* of linking or associating with the Google accounts of specific individuals, using cookies, IP addresses, and user agent data on its own, or by leveraging one of the many, off-the-shelf identity resolution services. (Shafiq Exp. Rpt. (dkt. #88, ¶ 14); Shafiq Supp. Exp. Rpt. (dkt. #161, ¶ 11).) However, as defendants point out, plaintiffs offer no evidence from which this court or a reasonable jury could conclude that their patient identity or other PHI was *actually* disclosed to Google, much less disclosed by or used by Google inappropriately. At most, plaintiffs' evidence establishes that the disclosed information included only anonymous device and account identifiers, while plaintiffs have *not* shown that these were actually used by Google or another third party to identify them. *See Doe v. Adventist Health Care Network, Inc.*, No. 22STCV36304, 2025 WL 1797226, at *9 (Cal. Super. Feb. 14, 2025) (denying class certification in similar tracking technology case without evidence that Google and Facebook actually accessed medical information as URL "containing a string of numbers and letters does not, on its face, reveal medical information").

While Dr. Shafiq has now clarified in his supplemental report that "Google can *and did* use identifying information collected from patients as a result of [HSHS's] and Prevea's installation and use of tracking technologies from Google to link that information to specific individuals, including Plaintiffs" (dkt. #161, ¶ 20(c) (emphasis added)), he does not identify any evidence or examples of this actually occurring. Instead, Dr. Shafiq's supplemental report explains:

[13] This information included either full-string page URLs and page titles in the case of website logins, or app events and screen names in the case of MyPrevea's Android app, all of which Dr. Shafiq says showed the substance of patients' interactions with the portal, including information about patient status, patient appointments, lab results, and bill payment. (*Id.*; dkt. #161, ¶ 30.)

- Google's own public documentation states that it *may* associate activity on other sites and apps with personal information in order to improve Google's services and the ads delivered by Google, and *may* make that activity available to third-party advertising technology providers. (*Id.*, ¶ 36 (emphasis added).)

- Each of these identifiers is independently *capable* of enabling user identification or association, and Google's systems are in fact designed to, and do, use them in combination. This impacted Plaintiffs because they each confirmed they accessed Defendants' portals after authenticating themselves during the class periods relevant to each Plaintiff. There is no evidence the tracking technology erred, malfunctioned, or failed to work in any way that would have prevented the transfer of Plaintiffs' data to Google. (*Id.*, ¶ 38 (emphasis added).)

- "Google's own documentation, along with my own testing and analysis, confirms that it uses information collected across sites and apps that partner with Google, such as Hospital Sisters and Prevea using Google Analytics, and that such activity is associated with a user's Google account. As a result, when Hospital Sisters and Prevea shared identifying information and content information to Google through Google Analytics, Google had both the technical capability and the documented practice of linking that information to specific individuals using cookies and other identifying information." (*Id.*, ¶ 44.)

Thus, even though Dr. Shafiq states that "[f]rom a technical standpoint, Google Analytics cannot function as an analytics system without first distinguishing individual users or devices" (*id.*, ¶ 42), he fails to present any evidence from which this court or a jury could reasonably conclude that Google actually took the next step of identifying the named plaintiffs, much less the thousands of putative class members. Further, as defendants also point out, neither Dr. Shafiq nor plaintiffs have offered evidence that *defendants* versus other third parties (or even plaintiffs themselves based on their own voluntary internet disclosures)[14] caused plaintiffs' PHI to be shared so as to explain plaintiffs receiving advertising targeted to their particular medical conditions.

[14] It is undisputed that the named plaintiffs have either shared or researched their health conditions online, or been the target of a data breach or another provider's tracking technology.

As the Seventh Circuit held in *Dinerstein*, 73 F.4th at 502 (7th Cir. 2023), this is a factual distinction with a legal difference. In *Dinerstein*, a patient at a university hospital, whose anonymized electronic health records had been disclosed for research purposes to Google to create predictive health models, filed a putative class action claiming injury based on various privacy, contractual, tortious-interference, and consumer-fraud laws. *Id*. at 507-08. However, the Seventh Circuit dismissed the case for lack of standing at the motion to dismiss stage, finding it significant that Dinerstein had neither alleged that any specific identifying information had evaded redaction, nor that Google had taken any steps to identify him in the past or intended to do so in the future. *Id*. at 513-15; *see also id*. at 513 ("Dinerstein has identified no case in which a court has permitted a plaintiff to bring a public-disclosure tort premised on the dissemination of anonymized information. Indeed, while the relevant caselaw is sparse, we're skeptical that this alleged factual scenario would give rise to any injury at all -- let alone one concrete enough to support Article III standing."); *id*. at n.2 ("Nor has Dinerstein identified a case in which a court has permitted a plaintiff to bring the novel claim of breach of medical confidentiality in circumstances like these.").

Nevertheless, unlike the plaintiff in *Dinerstein*, this court allowed the original named plaintiff, Brahm, to proceed past the motion to dismiss stage because she had alleged that: personal medical information defendants disclosed to Google and Facebook was *not* anonymized; and those advertisers not only designed various ways to gain access to identifying information for patients, but had all the information needed to identify individual patients on defendants' websites. *Brahm*, 2024 WL 3226135, at *4. At the pleading stage, this court explained that the truth of those factual allegations were best resolved at summary judgment or trial. *Id*.

Now, with the benefit of a full record, plaintiffs have failed to present actual evidence that Google took any steps to identify plaintiffs individually, nor even that it intends to do so in the future. *See Pierre*, 29 F.4th at 938 ("A plaintiff seeking money damages has standing to sue in federal court only for harms that have in fact materialized."); *In re Hulu Priv. Litig.*, No. C 11–03764 LB, 2014 WL 1724344, at *12 (N.D. Cal. Apr. 28, 2014) (granting summary judgment where plaintiffs' theory of harm was based on "the hypothetical" that a third party could "reverse engineer" unique user IDs to determine website visitors' names); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) ("Although Plaintiffs postulate that these third parties could, through inferences, de-anonymize [LinkedIn] data, it is not clear that anyone has actually done so, or what information, precisely, these third parties have obtained."). Thus, plaintiffs have not supported either allegation that arguably, previously differentiated their claims from the plaintiff in *Dinerstein*.

Plaintiffs now attempt to distinguish *Dinerstein* on the grounds that the research contract between that hospital and Google expressly *prohibited* Google from attempting to identify any patient whose records were disclosed for research purposes; while in this case, *identifying and distinguishing* patients is allegedly the very object of Google Analytics, plaintiffs must still present sufficient evidence that Google Analytics actually worked as allegedly intended, which they have failed to do in this case. Accordingly, plaintiffs have failed to show any injury in fact at all, let alone one concrete enough to support standing for claims of compensatory (or even nominal) damages under Article III.

In addition, to the extent that plaintiffs may claim to be pursuing forward-looking, injunctive relief to prevent a privacy injury from occurring in the future, the alleged risk that Google or any other third party may identify plaintiffs at a later date by leveraging any data

that it obtained from defendants is not sufficiently imminent to obtain injunctive relief in federal court. *Dinerstein*, 73 F.4th at 515 (Dinerstein's "highly speculative fear" that Google might identify him at some point in the future was "nowhere near 'certainly impending'" and "too speculative to satisfy the imminence requirement for a suit for injunctive relief in federal court.").

B. Breach of Implied Contract

While the parties did not enter into an express, written contract with respect to plaintiffs' PHI, they separately claim that defendants breached *implied* contracts entered into with plaintiffs "for the provision of medical care and treatment, which included an implied agreement for Defendants to retain and protect the privacy" of plaintiffs' PHI. (Amd. Cpt., dkt. #51, at ¶¶ 281-82.) In Wisconsin, "[a]n implied-in-fact contract is a meeting of the minds that is circumstantially proved by words and conduct which show a mutual intention to contract." *M&D Truck & Equip. Sales LLC v. Daniel Amarei*, No. 2024AP2083, 2026 WL 835952, at *12 (Wis. Ct. App. Mar. 26, 2026) (citing *Theuerkauf v. Sutton*, 102 Wis. 2d 176, 306 N.W.2d 651 (1981); WIS JI-CIVIL 3024 ("An agreement may be established by the conduct of the parties . . . if from such conduct it can fairly be inferred that the parties mutually intended to agree on all terms.")).[15] Here, plaintiffs contend that: (1) defendants "solicited and invited [plaintiffs] to provide their PII/PHI on their websites as part of Defendants' regular business practices"; (2) plaintiffs accepted defendants offers and provided their PHI to

[15] While Wisconsin recognizes both contracts implied-in-fact and implied-in-law, only implied-in-fact contracts rely on the contract-formation and breach principles, which plaintiffs rely on in asserting this claim. *See Lindquist Ford, Inc. v. Middleton Motors, Inc.*, 557 F.3d 469, 481 (7th Cir. 2009).

defendants as part of acquiring defendants' medical services; and (3) "[p]er their contractual, legal, ethical, and fiduciary duties, Defendants were obligated to take adequate measures to protect [plaintiffs'] PII/PHI from unauthorized disclosure to third parties," which they failed to do. (*Id.*, at ¶ 281.)

However, plaintiffs' asserted pecuniary harm based on either the diminished sales value of their PHI or nominal damages fails for the same reasons discussed above in conjunction with their tort claims. In addition, any argument that plaintiffs may have that defendants' breach of contract is itself a legally cognizable, injury-in-fact is a nonstarter because the Seventh Circuit has already held that "a breach of contract alone -- without any actual harm -- is purely an injury in law, not an injury in fact," falling short of Article III standing. *Dinerstein*, 73 F.4th at 522; *see also TransUnion*, 594 U.S. at 427 (holding that "an injury in law is not an injury in fact" in distinguishing between a cause of action giving right to sue and any injury suffered as a result). Thus, plaintiffs cannot satisfy the injury-in-fact requirement of Article III without proof that defendants' purported breach of contract actually resulted in some concrete harm, which they have wholly failed to do so.

C. Unjust Enrichment

In alternative to their claims for breach of contract implied-in-fact, named plaintiffs Brahm, Quaid, Ward, and Bornemann[16] -- on behalf of themselves only -- assert claims of

[16] Specifically, Brahm and Quaid assert this claim against HSHS, while Ward and Bornemann assert this claim against both HSHS and Prevea.

unjust enrichment, which Wisconsin sometimes refers to as a contract implied-in-law.[17] *See Mohns Inc. v. BMO Harris Bank Nat'l Ass'n*, 2021 WI 8, ¶ 48, 395 Wis. 2d 421, 954 N.W.2d 339 ("Under Wisconsin law, a plaintiff may not recover damages for both breach of contract and unjust enrichment based on the same conduct. Unjust enrichment is an equitable claim that cannot coexist with a breach of contract claim.") (internal citations omitted). A claim for unjust enrichment requires proof that plaintiffs conferred a benefit on defendants, with defendants' knowledge or appreciation, which is inequitable for defendants to accept or retain without payment of its value. *Admiral Ins. Co. v. Paper Converting Mach. Co.*, 2012 WI 30, ¶ 46 n.16, 339 Wis. 2d 291, 811 N.W.2d 351 (citing Wis JI-Civ 3028). "The measure of damages under unjust enrichment is limited to the value of the benefit conferred on the defendant." *Lindquist*, 557 F.3d at 477.

Here, plaintiffs claim that defendants collected and unjustly retained without compensation plaintiffs' "valuable and sensitive medical information," under the guise of keeping this information private, then disclosed this information to third parties for defendants' own gain, including advertising and other "valuable services." (Dkt. #51, at ¶ 337.) Plaintiffs seek to measure that benefit by showing that defendants' misuse diminished the value of their PHI, which is a "reasonable proxy for the benefit" defendants retained for themselves. (Dkt. #157, at 31.) However, as explained above, without any evidence of

[17] The terminology associated with contracts implied-in-law is admittedly confusing: while Wis JI-Civ 3028 is titled "Contracts Implied in Law (Unjust Enrichment)," the "Wisconsin Supreme Court distinguishes 'quantum meruit/contracts implied by law' from 'unjust enrichment,' where there is no implied contract at all." *Lindquist*, 557 F.3d at 480. Here, the named plaintiffs have made clear that their alternative claim is one for unjust enrichment, as they do not discuss quantum meruit, which relates to the *performance* of valuable *services* for which no compensation was received. *Id*. at 478.

improper disclosure, this alleged pecuniary injury is simply speculative and insufficient to confer standing.

D. Wiretapping Claims

Finally, plaintiffs' wiretapping claims turn on whether defendants intercepted their PHI without consent for a tortious, criminal, or injurious purpose. Specifically, the Federal Wiretap Act, 18 U.S.C. § 2511, prohibits any person from intentionally disclosing or using "the contents" of any "electronic communication" 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." Wisconsin's wiretapping statute, Wis. Stat. § 968.31, provides even broader protections than its federal counterpart by prohibiting a party to the communication from intercepting contents for the purpose of committing any "injurious act," which courts have interpreted to mean any conduct that could harm claimants, as evaluated on a case-by-case basis. *See State v. Waste Mgmt. of Wis., Inc.*, 81 Wis. 2d 555, 571 and n.17, 261 N.W.2d 147 (1978) (citing and quoting *Meredith v. Gavin*, 446 F.2d 794, 799 (8th Cir. 1971)).

Plaintiffs purport to satisfy the illicit purpose element of these claims under federal and state laws by arguing that defendants committed independent torts, crimes, and injurious acts by tracking their patients without consent. *E.g.*, *Hartley v. University of Chicago Medical Ctr.*, 2025 WL 2802317, at *9 (N.D. Ill. Oct. 1, 2025) ("Hartley alleges that UCMC's disclosure of her health information violated HIPAA, so she has alleged a criminal or tortious purpose independent of the interception of her information"). However, as discussed above, plaintiffs have failed to present evidence showing that the information received and disclosed by defendants caused any injury-in-fact. Further, while plaintiffs seek statutory damages for their

wiretap claims, a statutory violation does not, on its own, convey standing absent an underlying concrete, particularized injury. *TransUnion*, 594 U.S. at 427 ("Only those plaintiffs who have been concretely harmed by a defendant's statutory violation may sue that [] defendant over that violation in federal court."); *Spokeo,* 578 U.S. at 341 ("Article III standing requires a concrete injury even in the context of a statutory violation."); *Markakos v. Medicredit, Inc.*, 997 F.3d 778, 780-81 (7th Cir. 2021) (collecting cases holding that "precedent . . . faithfully holds that a statutory violation alone does not cause an injury in fact").

III. Remand

For all of these reasons, plaintiffs do not have standing in this federal court with respect to any of their claims for relief. Accordingly, this case will be remanded to state court for further proceedings under 28 U.S.C. § 1447(c). *See Collier v. SP Plus Corp.*, 889 F.3d 894, 896 (7th Cir. 2018) (Section 1447(c) "makes clear that the district court must remand the case to state court if 'at any time before final judgment it appears that the district court lacks subject matter jurisdiction.'"). While § 1447(c) further provides for "payment of just costs and any actual expenses, including attorney fees, incurred as a result of the removal," an award of fees is appropriate only where the removing party lacked an "objectively reasonable basis" for seeking removal. *Martin v. Franklin Cap. Corp.*, 546 U.S. 132, 141 (2005).

The Seventh Circuit describes this general rule as follows: "if, at the time the defendant filed his notice in federal court, clearly established law demonstrated that he had no basis for removal, then a district court should award a plaintiff his attorneys' fees. By contrast, if clearly established law did not foreclose a defendant's basis for removal, then a district court should not award attorneys' fees." *Wolf v. Kennelly*, 574 F.3d 406, 412 (7th Cir. 2009) (citing *Lott v.*

Pfizer, Inc., 492 F.3d 789, 793 (7th Cir. 2007). Here, clearly established law did not foreclose removal because, as this court previously held, the *allegations* in plaintiffs' initial and amended complaints alleged an injury-in-fact. Plaintiffs' lack of standing only became clear as this case moved beyond the pleading stage and it became apparent that plaintiffs had insufficient evidence of a legally-cognizable injury in fact. Accordingly, the court will not award attorney's fees against the defendants in this case.

ORDER

IT IS ORDERED that:

1. This case is REMANDED to the Eau Claire County Circuit Court for lack of subject matter jurisdiction, and the clerk of court is directed to return the record to that court.

2. Plaintiffs' motion to strike the expert report of James Vint (dkt. #120), defendants' motion to strike the expert opinion of Eric Krause (dkt. #129), plaintiffs' motion for class certification (dkt. ##68, 90), and defendants' motion for summary judgment (dkt. #131) are DENIED as moot.

Entered this 1st day of May, 2026.

BY THE COURT:

/s/

_____
WILLIAM M. CONLEY
District Judge