

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

ARNOLD STEIN, <i>et al.</i> ,)	
)	
Plaintiffs,)	Case No. 23-cv-14515
)	
v.)	Hon. Steven C. Seeger
)	
EDWARD-ELMHURST HEALTH,)	
)	
Defendant.)	
_____)	

MEMORANDUM OPINION AND ORDER

Arnold Stein and Diane Miller shared their medical information with Edward-Elmhurst Health, using a web-based portal called MyChart. They believed that their communications were confidential, and that Edward-Elmhurst Health would protect the privacy of their health information. They were none too pleased to discover that the website contains an embedded software that automatically transmits their information to Facebook.

So they sued. Stein and Miller filed a complaint on behalf of themselves and a putative class, bringing eight claims. Edward-Elmhurst Health moved to dismiss the complaint in its entirety. And in response, Stein and Miller came to the defense of only three claims.

For the reasons stated below, the motion to dismiss is granted in part and denied in part.

Background

At the motion to dismiss stage, the Court must accept as true the well-pleaded allegations of the complaint. *See Lett v. City of Chicago*, 946 F.3d 398, 399 (7th Cir. 2020). The Court “offer[s] no opinion on the ultimate merits because further development of the record may cast the facts in a light different from the complaint.” *Savory v. Cannon*, 947 F.3d 409, 412 (7th Cir. 2020).

If you had to pick the favorite word in the Federal Rules of Civil Procedure of most district court judges, “short” would be a good bet. *See* Fed. R. Civ. P. 8(a)(1). The Federal Rules simply require a “short and plain” statement of a claim showing that the claimant is entitled to relief. *Id.*

That admonition exists for good reason. The Federal Rules contemplate notice pleading. A complaint simply needs to put the ball in play by giving notice to the other side of the nature of the claim, supported by enough facts to give rise to a plausible claim. Long complaints add complexity to the case from the get-go, and impose significant burdens on the responding party. Everyone likes brevity when someone else is doing the talking.

Sometimes complaints stretch the boundaries of “short,” especially in complex cases. It is a challenge to convey complicated factual scenarios in a small amount of words. *But see* President Abraham Lincoln, *The Gettysburg Address* (Nov. 19, 1863).

Other factors might create a temptation to draft a long complaint. Sometimes plaintiffs put lots of cards on the table to show that they have their ducks in a row, and have the goods on the defendants. A long complaint might have educational value for an uninformed reader, too (like a judge who doesn’t know the background). And there might be some rhetorical benefit in telling your story from the get-go, even if it’s a long-winded story.

Most of the time, district court judges aren’t in the business of enforcing the rule about short pleadings, probably because of the shortness of time. It is rare to dismiss a complaint for being too long, although the thought undoubtedly crosses judicial minds.

Here, Plaintiffs filed a complaint that weighs in at 106 pages. That’s not exactly “short.” It is more than enough to create multiple squadrons of paper airplanes.

The 106-page, 448-paragraph complaint asserts eight claims. Lots of the paragraphs offer a deep dive into the underlying technology. The complaint isn't "short," but this Court will offer a short summary of a long complaint.

Edward-Elmhurst Health ("EEH") is a health care provider with dozens of locations in Illinois. EEH owns, controls, and maintains a website that patients use to book medical appointments, communicate medical symptoms, and more. *See* Am. Cplt., at ¶ 6 (Dckt. No. 31). EEH also maintains a web-based portal called MyChart, where users can communicate with doctors, access test results, manage prescription and appointments, and more. *Id.* at ¶ 7. The parties refer to the website and portal as the "web properties." *Id.* at ¶ 8.

Arnold Stein, Diane Miller, and the putative class members (collectively, "Plaintiffs") used the web properties. Plaintiffs thought they were communicating only with their healthcare providers. *Id.* at ¶ 9.

Unbeknownst to them, EEH had embedded a software called the Meta Tracking Pixel on its web properties. *Id.* at ¶ 10. The Pixel "automatically transmits to Facebook every click, keystroke, and detail about their medical treatment." *Id.*

That information is disclosed to Facebook along with the person's unique Facebook ID. So Facebook can instantly associate someone's personal health data with a specific Facebook user. *Id.* at ¶¶ 11–12.

In addition to the Pixel, EEH installed Facebook's Conversions Application Programming Interface ("CAPI") on its website. *Id.* at ¶ 16. CAPI is a bit different from the Pixel. The Pixel coopts a website user's browser and forces it to disclose information to Facebook as well as to EEH. *Id.* at ¶ 17. But CAPI tracks the user's website interactions. CAPI then records and stores

that information on EEH's servers, and then transmits the data to Facebook from EEH's servers.
Id.

In short, if you use EEH's web properties, Facebook knows everything you put into the web properties.

Plaintiffs allege that EEH decided to use the Pixel and CAPI "for marketing purposes in an effort to bolster [EEH's] profits." *Id.* at ¶¶ 20–21. EEH wanted to exploit the personal health data of the patients to "increase its ability to market and retarget its [u]sers, thereby increasing its profit." *Id.* at ¶ 29.

Plaintiffs were not aware that EEH was transmitting their information to Facebook while they communicated with their healthcare providers on the web properties. And they didn't know that their information was stored on EEH's servers to be transmitted to Facebook later for targeted advertising and marketing purposes. *Id.* at ¶ 30.

In fact, they had the opposite understanding. EEH "broadly proclaimed . . . the lengths it will supposedly go to protect its patients' personal and protected health information." *Id.* at ¶ 1.

So Plaintiffs sued EEH. They brought eight claims: (1) violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2511(1), *et seq.*; (2) violation of the Illinois Eavesdropping Statute, 720 ILCS 5/14-1, *et seq.*; (3) violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*; (4) violation of the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS 510/2, *et seq.*; (5) breach of confidence; (6) common law invasion of privacy, for intrusion upon seclusion; (7) breach of implied contract; and (8) negligence. *Id.* at ¶¶ 335–448.

EEH moved to dismiss the complaint for failure to state a claim. *See Mtn. to Dismiss* (Dckt. No. 38).

Legal Standard

A motion to dismiss under Rule 12(b)(6) challenges the sufficiency of the complaint, not its merits. *See* Fed. R. Civ. P. 12(b)(6); *Gibson v. City of Chicago*, 910 F.2d 1510, 1520 (7th Cir. 1990). When considering a Rule 12(b)(6) motion to dismiss, the Court accepts as true all well-pleaded facts in the complaint and draws all reasonable inferences from those facts in the plaintiff's favor. *See AnchorBank, FSB v. Hofer*, 649 F.3d 610, 614 (7th Cir. 2011).

To survive a Rule 12(b)(6) motion, the complaint must provide the defendant with fair notice of the basis for the claim, and it must be facially plausible. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *See Iqbal*, 556 U.S. at 678.

Analysis

Plaintiffs brought eight claims, but most of them didn't get very far. EEH moved to dismiss all eight claims, and in response, Plaintiffs came to the defense of only three of them. Plaintiffs have abandoned five of the eight claims, so they are dismissed. *See G & S Holdings LLC v. Continental Cas. Co.*, 697 F.3d 534, 538 (7th Cir. 2012).

Only three claims remain. The first claim is a federal claim under the Electronic Communications Privacy Act (Count I). The second claim is a state-law claim under the Illinois Eavesdropping Statute (Count II). The last remaining claim is a negligence claim (Count VIII).

I. The Electronic Communications Privacy Act (Count I)

The first claim falls under the Electronic Communications Privacy Act (“ECPA”), which courts sometimes call the Wiretap Act. The statute makes it unlawful to “intentionally

intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.” *See* 18 U.S.C. § 2511(1)(a).

The elements of a claim jump off the page. A plaintiff must show that the 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.” *See In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 135 (3d Cir. 2015). The word “intercept” sweeps broadly, covering “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” *See* 18 U.S.C. § 2510(4).

The ECPA has an exception: the so-called one-party consent rule. Under that rule, it is not unlawful for a party to intercept *its own* communications. “It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception *unless* such 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.” *See* 18 U.S.C. § 2511(2)(d) (emphasis added).

But the exception has a few twists and turns. It includes a carve-out, as revealed by the phrase that begins with “unless.” The one-party consent rule does not apply if “such 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.” *Id.*

The crime or tort can’t be the interception itself. “To survive a motion to dismiss, a plaintiff must plead sufficient facts to support an inference that the offender intercepted the

communication for the purpose of a tortious or criminal act that is *independent* of the intentional act of recording.” See *Caro v. Weintraub*, 618 F.3d 94, 97 (2d Cir. 2010) (emphasis in original); see also *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d at 145. There is no double dipping – the conduct must violate something else for the crime-tort exception to apply.

Putting it all together, the ECPA makes it unlawful to intentionally intercept communications. But a party to the conversation is free to intercept its own communications, unless it does so for the purpose of committing an act that is a crime or a tort. And the crime or tort cannot be the interception itself.

To illustrate the statute, consider a hypothetical about jaywalking. Imagine if the City of Chicago banned jaywalking, with one exception. Imagine if the City of Chicago allowed jaywalking if a person is by himself, unless that person jaywalks for the purpose of committing a crime or tort.

Suppose that the Joker jaywalked by himself for the purpose of robbing Gotham Bank across the street. In that scenario, the “crime or tort” is not the jaywalking. The crime or tort is the bank robbery. So the carve-out to the exception would apply. And Commissioner Gordon could give the Joker a ticket for jaywalking (in addition to arresting him for robbing the bank).

But imagine if the Joker jaywalked by himself for the purpose of saying hello to the Penguin across the street. Saying hello to the Penguin is not a crime or a tort. So, the carve-out to the exception would not apply. In that situation, the Joker would not violate the jaywalking ordinance – he jaywalked, but he was by himself, and he didn’t jaywalk to commit a crime or tort.

Here, Plaintiffs allege that EEH violated the Health Insurance Portability and Accountability Act (popularly known as “HIPAA”), because EEH disclosed their individually identifiable health information to a third party. *See* Am. Cplt., at ¶¶ 353–55. That statute imposes a criminal penalty for knowingly “disclosing individually identifiable health information to another person.” *See* 42 U.S.C. § 1320d-6(a)(3).

A disclosure that violates HIPAA is a violation of law that is independent of a violation of the ECPA. That’s enough to conclude that the crime-tort exception applies. That is, the crime-tort exception to the one-party consent rule applies, because a violation of HIPAA is a crime or tort.

Courts in this district have recognized that disclosing health information in violation of HIPAA can provide the predicate for a claim under the ECPA. *See A.D. v. Aspen Dental Mgmt., Inc.*, 2024 WL 4119153, at *3 (N.D. Ill. 2024) (“Accepting Plaintiffs’ allegations as true, as the Court must at this stage, Aspen placed tracking technology on its website with the intent to collect and disclose users’ personal health information for purposes of financial gain, in violation of [HIPAA] Plaintiffs plausibly allege that [Defendant] intended to violate the HIPAA when it transmitted Plaintiffs’ information to third parties, which is distinct from the improper interception.”); *Kurowski v. Rush System for Health*, 2023 WL 8544084, at *3 (N.D. Ill. 2023) (“*Rush III*”) (holding that allegations of sharing medical information were “sufficient to invoke the HIPAA exception-to-the-party-exception” of the ECPA); *Smith v. Loyola Univ. Med. Ctr.*, 2024 WL 3338941, at *7 (N.D. Ill. 2024) (“Such [health] information qualifies as IIHI for purposes of HIPAA. . . . Further, the plaintiffs allege that LUMC’s collection and disclosure of their personal health information was done knowingly and for purposes of financial gain –

namely, to bolster profits via targeted marketing campaigns. . . . Taken as a whole, these allegations are sufficient to invoke HIPAA for purposes of the ECPA’s crime-tort exception.”).

Courts from coast to coast have recognized that a violation of HIPAA can give rise to the crime-tort exception under the ECPA. *See, e.g., Kane v. University of Rochester*, 2024 WL 1178340, at *7 (W.D.N.Y. 2024) (“This Court likewise concludes that Plaintiffs can invoke the tort-crime exception. Plaintiffs have alleged that Defendant configured the Pixel to collect and disclose, among other things, that a specific user booked an appointment with a specific healthcare provider and the search terms that the user entered to find that provider. . . . They have further alleged that Defendant disclosed this information to enhance its marketing efforts.”); *In re Grp. Health Plan Litig.*, 709 F. Supp. 3d 707, 719 (D. Minn. 2023); *Strong v. LifeStance Health Grp. Inc.*, 2025 WL 317552, at *5 (D. Ariz. 2025); *Castillo v. Costco Wholesale Corp.*, 2024 WL 4785136, at *7 (W.D. Wash. 2024); *Gay v. Garnet Health*, 2024 WL 4203263, at *3–4 (S.D.N.Y. 2024); *Sweat v. Houston Methodist Hosp.*, 2024 WL 3070184, at *4 (S.D. Tex. 2024).

EEH believes that the crime-tort exception does not apply because EEH did not intercept the communications for the purpose of committing a crime or tort. Instead, the complaint alleges that EEH intercepted the communications to make money. *See* Am. Cplt., at ¶¶ 21, 22, 29, 51, 69, 85, 92, 137, 278, 281 (Dckt. No. 31); Def.’s Reply, at 4–5 (Dckt. No. 43).

To be sure, some courts have concluded that the crime-tort exception does not apply when the underlying motivation is financial, not criminal or tortious. *See, e.g., In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 797 (N.D. Cal. 2022) (“Multiple 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, not to injure plaintiffs tortiously.”); *Katz-Lacabe v. Oracle America, Inc.*, 668 F. Supp. 3d 928, 945 (N.D. Cal. 2023) (“Plaintiffs’ attempt to invoke

the crime-tort exception, requiring them to plead sufficient facts to show that ‘the primary motivation or a determining factor in the interceptor’s actions has been to injure plaintiffs tortiously,’ does not apply to a case such as this, where Defendant’s ‘purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money.’”) (citation omitted); *Rodriguez v. Google LLC*, 2021 WL 2026726, at *6 n.8 (N.D. Cal. 2021); *In re Google Inc. Gmail Litig.*, 2014 WL 1102660, at *18 n.13 (N.D. Cal. 2014) (“[T]he tort or crime exception cannot apply where the interceptor’s ‘purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money.’”) (citation omitted); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 519 (S.D.N.Y. 2001) (“DoubleClick’s purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money by providing a valued service to commercial Web sites.”); *but see In re Grp. Health Plan Litig.*, 709 F. Supp. 3d at 720 (“[T]his district has not found that the crime-tort exception to the Wiretap Act is inapplicable where the defendant’s primary motivation was to make money.”).

That approach seems difficult to square with the statutory text. The language of the statute gives no hint that conduct falls outside the reach of the statute if a person acted based on financial motivations.

Again, the crime-tort exception to the one-party consent rule applies if a defendant intercepts the communication “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.” *See* 18 U.S.C. § 2511(2)(d). A party does not have to say, in effect, “I want to commit a crime,” or “today is a great day to commit a tort.”

The text points to the “purpose of committing any criminal or tortious *act*.” *Id.* (emphasis added). Separating the adjectives from the noun might shed a little light. The purpose

must be to commit an act, and that act must be criminal or tortious. If the purpose is to do X, and if X is a crime or a tort, then the crime-tort exception to the one-party consent rule applies. A desire to commit a crime *qua* crime, or a tort *qua* tort, isn't necessary.

The placement of “criminal or tortious” is telling. That phrase modifies “act,” not “purpose.” The statute does not require a “criminal or tortious purpose.” It requires a purpose of committing an act – an act that is criminal or tortious.

A person can have a purpose of committing an act that is criminal or tortious, without having a criminal or tortious purpose. Imagine changing lanes on the highway without looking, and nailing the car in the other lane. The bad driver may have acted with the purpose of committing an act – changing lanes – that was tortious (because of the lack of ordinary care). But that's different than saying that the driver acted with a tortious purpose.

The other reading would, in effect, import a *mens rea* element into the statute. Congress could have required a showing that the person acted with a criminal or tortious purpose. The text could have covered intercepting a communication “for a criminal or tortious purpose.” Or, the statute could have applied to intercepting a communication “for a criminal or tortious purpose to commit a criminal or tortious act.”

But that's not what the text says. The “act” must be criminal or tortious, but the “purpose” does not need to be criminal or tortious.

Even if the carve-out required a criminal or tortious purpose, it would be odd to exclude an otherwise criminal or tortious act solely because it was also motivated by financial gain. The existence of an underlying financial motivation does not mean that the act lacked a criminal or a tortious purpose. That's like saying that a bank robber's purpose was not to commit a crime – it was to make money.

The existence of a financial motivation (on the one hand) and a criminal or tortious motivation (on the other hand) are not mutually exclusive. After all, lots of crimes and torts are money-makers. Crime pays (until it doesn't), and lots of torts are good for the bottom line, too. The annals of history are chock-full of villains who have a financial motivation – Madoff, Dr. Evil, and Al Capone, to name a few.

One has to wonder if an exception for financial motivations would sweep too broadly, and swallow the rule. After all, a drive to make money is an all-too-human, hard-to-avoid motivation. It is inescapable, and helps make the world go round.

As this Court sees things, the existence of a financial motivation is not a get-out-of-liability-free card. The statute does not exclude conduct simply because someone acted with a financial purpose.

Here, the complaint alleges that EEH disclosed Plaintiffs' health information to a third party in violation of 42 U.S.C. § 1320d-6(a)(3). That's enough to get around the ECPA's one-party consent rule, because the crime-tort exception applies. The motion to dismiss the claim under the ECPA is denied.

II. The Illinois Eavesdropping Statute (Count II)

The second claim falls under the Illinois Eavesdropping Statute. Plaintiffs allege that EEH violated two subparts of that statute.

First, Plaintiffs assert that EEH violated section 5/14-2(a)(2), which prohibits using “an eavesdropping device, in a surreptitious manner, for the purpose of transmitting or recording all or any part of any private conversation to which he or she is a party unless he or she does so with the consent of all other parties to the private conversation.” *See* 720 ILCS 5/14-2(a)(2); Am. Cplt., at ¶ 358 (Dckt. No. 31).

EEH moved to dismiss the claim under that provision, arguing that it applies only to oral communications. The Court agrees.

Section 5/14-2(a)(2) uses the phrase “private conversation.” *See* 720 ILCS 5/14-2(a)(2). The statute defines the phrase “private conversation” to mean “any oral communication between 2 or more persons.” *See* 720 ILCS 5/14-1(d). Only “oral” communications count.

Plaintiffs don’t allege that EEH transmitted or recorded an oral communication, so that provision does not come into play.

Plaintiffs point to an amendment of the statute in 2014. The Illinois legislature amended the “private conversation” language to include communications “transmitted between the parties by wire or other means.” *See* Pls.’ Mem. in Opp., at 14 (Dckt. No. 41). As Plaintiffs see things, the meaning of “private conversation” is “clearly not restricted to oral conversations only.” *Id.*

That’s not what the statute says. Even after the 2014 amendment, the statute says that a “private conversation” means “any oral communication between 2 or more persons, in person or transmitted between the parties by wire or other means.” *See* 720 ILCS 5/14-1(d). If the communication isn’t “oral,” it doesn’t give rise to a claim under section 5/14-2(a)(2).

Second, Plaintiffs assert that EEH violated section 5/14-2(a)(5) of the eavesdropping statute. That provision makes it unlawful to “[u]se[] or disclose any information which he or she knows or reasonably should know was obtained from a private conversation or private electronic communication in violation of this Article, unless he or she does so with the consent of all the parties.” *See* 720 ILCS 5/14-2(a)(5); Am. Cplt., at ¶ 360 (Dckt. No. 31).

Section 5/14-2(a)(5) provides two potential sources for private information: “private conversation[s]” and “private electronic communication[s].” *See* 720 ILCS 5/14-2(a)(5). The

complaint does not get nitty gritty, and specify which route Plaintiffs plan to take. But either way, they hit a dead end.

Plaintiffs cannot go the “private conversation” route, because they hit the same roadblock as before. A private conversation is an oral communication, and the complaint does not allege that EEH disclosed an oral conversation. *See* 720 ILCS 5/14-1(d).

Plaintiffs cannot get anywhere by going down the road of a “private electronic communication[s],” either. A “private electronic communication” means “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation.” *See* 720 ILCS 5/14-1(e).

Section 5/14-2(a)(5) comes with a hitch. That provision does not simply prohibit the use or disclosure of information from private electronic communications. It prohibits the use or disclosure of information from private electronic communications “obtained . . . in violation of this Article.” *See* 720 ILCS 5/14-2(a)(5).

So, based on the statutory text, it is not enough for the information to come from private electronic communications. The text prohibits the use or disclosure of information if the person “knows or reasonably should know” that the information “was obtained from a private conversation or private electronic communication *in violation of this Article.*” *Id.* (emphasis added).

That subpart presupposes that the information was collected “in violation of this Article.” *Id.* And that’s where the complaint at hand runs into trouble.

The statute's first four subparts list the four ways that a person can obtain information in violation of the statute. But none applies to this case. So EEH did not "obtain [information] from a . . . private electronic communication in violation of this Article." *Id.*

The complaint does not allege that EEH used an "eavesdropping device." *See* 720 ILCS 5/14-2(a)(1), (2). And EEH did not manufacture, assemble, distribute, or possess any eavesdropping device or comparable device, either. *See* 720 ILCS 5/14-2(a)(4).

That leaves section 5/14-2(a)(3) as the last provision standing. That provision applies when a party intercepts, records, or transcribes a private electronic communication "to which he or she is not a party unless he or she does so with the consent of all parties to the private electronic communication." *See* 720 ILCS 5/14-2(a)(3). But here, EEH was a party to the communications.

In sum, the complaint does not allege a violation of section 5/14-2(a)(5). It does not allege that EEH intercepted an oral communication. And it does not allege that EEH used or disclosed information obtained in violation of the statute. So it does not state a claim.

The claim under the Illinois Eavesdropping Statute (Count II) is hereby dismissed.

III. Negligence (Count VIII)

The last remaining claim is a negligence claim. The elements are familiar: duty, breach, causation, and injury. A plaintiff "must plead that the defendant owed a duty of care to the plaintiff, that the defendant breached that duty, and that the breach was the proximate cause of the plaintiff's injuries." *See Cowper v. Nyberg*, 28 N.E.3d 768, 772 (Ill. 2015) (citation omitted).

EEH moves to dismiss based on a lack of a duty of care. As EEH sees things, the complaint does not allege a duty of care apart from physician-patient confidentiality, which is not

a basis for an independent tort claim under Illinois law. *See* Def.'s Mem., at 18–19 (Dckt. No. 39).

In response, Plaintiffs argue that there are two independent bases for a duty of care apart from the physician-patient relationship. *See* Pls.' Mem. in Opp., at 16 (Dckt. No. 41). First, EEH owed a duty to prevent disclosure of their private information to third parties. *Id.* Second, EEH assumed a duty to protect their private information by representing that it would not disclose that information without Plaintiffs' consent. *Id.*

As EEH sees things, Illinois law recognizes a common-law duty to prevent disclosure only for accidental data breaches, not for intentional disclosures. *See* Def.'s Reply, at 9 (Dckt. No. 43). EEH also balks at the notion that it assumed a duty to protect their information. In EEH's view, its "privacy policy disclaims any such duty." *See* Def.'s Resp. to Suppl. Authority, at 3 (Dckt. No. 51); *see also* Am. Cplt., Ex. A, at 3 (Dckt. No. 31-1) ("Edward-Elmhurst cannot ensure or warranty the security of any information you transmit to us, and you do so at your own risk.").

This Court will put to the side whether EEH assumed a duty of care by making representations about protecting privacy. Illinois recognizes a common-law duty of care.

Illinois law imposes a duty on data collectors to maintain reasonable security measures. *See Smith*, 2024 WL 3338941, at *7 (collecting cases); *see also* 815 ILCS 530/45(a) ("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.").

It's not "you buy it, you break it," but it's in the same neighborhood. You collect it, you keep it safe.

That duty is not limited to "allegations of data breach." *See Smith*, 2024 WL 3338941, at *7. It is not this Court's job to whittle down Illinois law, and create restrictions that Illinois courts themselves do not recognize. Federal courts take state law as they find it, and "it is not our role to break new ground in state law." *See Sabrina Roppo v. Travelers Com. Ins. Co.*, 869 F.3d 568, 596 (7th Cir. 2017) (quoting *Lopardo v. Fleming Cos., Inc.*, 97 F.3d 921, 930 (7th Cir. 1996)).

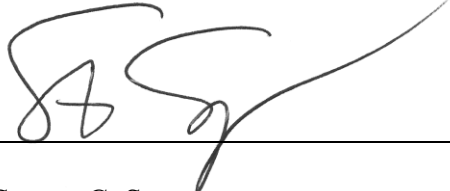
The complaint alleges that EEH collected Plaintiffs' sensitive medical information, and then disseminated that information to a third party without their consent. The collection of private health data is enough to give rise to a duty of care. *See Smith*, 2024 WL 3338941, at *7. A health provider that has private medical information in its hands must handle with care.

The motion to dismiss the negligence claim is denied.

Conclusion

For the foregoing reasons, Defendant's motion to dismiss is granted in part and denied in part. The Court denies the motion to dismiss the ECPA claim (Count I) and the negligence claim (Count VIII). All other claims are dismissed.

Date: February 21, 2025

A handwritten signature in black ink, appearing to read "S. Seeger", is written over a horizontal line.

Steven C. Seeger
United States District Judge