IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

EUGENE DIVISION

M.R.,[1]

Plaintiff,

v.

SALEM HEALTH HOSPITALS AND CLINICS,

Defendant.

Civ. No. 6:23-cv-01691-AA
OPINION & ORDER

AIKEN, District Judge.

Plaintiff is a patient of Defendant Salem Health Hospitals and Clinics and brings this putative class action arising out of Defendant's alleged disclosure of Plaintiff's confidential personally identifiable information. Before the Court is Defendant's Motion to Dismiss ("MTD"), ECF No. 9. For the reasons below, the Motion is GRANTED IN PART and COUNT FOUR of the Complaint is DISMISSED.

BACKGROUND

I. Factual and Procedural Background

Plaintiff is a former patient of Salem Health. Compl. at 1. Defendant is a healthcare entity and is subject to applicable HIPAA and Oregon law regulations on

[1] Plaintiff brings this lawsuit anonymously out of a desire to protect her personal health information under the Health Insurance Portability and Accountability Act of 1996 and Oregon law. Compl. at 2.

disclosing personally identifiable protected health information. Compl. ¶ 10, 13. Defendant owns and controls https://www.salemhealth.org ("Defendant's Website" or the "Website"), which it encourages patients to use for booking medical appointments, locating physicians and treatment facilities, communicating medical symptoms, searching medical conditions and treatment options, signing up for events and classes, and more. Compl. ¶ 3.

Plaintiff alleges that Defendant used hidden tracking tools embedded on its website, https://www.salemhealth.org, (the "Website"), Defendant Salem Health Hospitals and Clinics ("Salem" or "Defendant") intercepted Plaintiff's and Class Members' communications and forced their web browsers to send confidential and highly sensitive personally identifiable information ("PII") and personal health information ("PHI") (collectively, "Private Information") to undisclosed third parties such as Meta Platforms, Inc. ("Facebook") or Google, Inc. ("Google") without Plaintiffs' or Class Members' knowledge or consent. Compl. ¶¶ 5-6, 14, 54-58.

According to Plaintiff, the information Defendant intercepted and impermissibly disclosed to those third parties included booking of appointments, searches for specific medical treatment, particular health conditions, and other sensitive information. *Id*. Plaintiff asserts that Defendant used "Tracking Tools"—technology including Facebook Tracking Pixel ("Pixel"), Google Analytics, or Conversions API to boost its marketing efforts and profits by sharing Private Information despite protections offered to its patients through state and federal law and industry standards. *Id*. ¶¶ 44, 52-58. Plaintiff states that she used Defendant's

web portal and their website, https://www.salemhealth.org ("Website"), to research medical symptoms, search for doctors, make appointments, and check medical records. *Id.* at ¶ 7. Plaintiff maintains that her unique IP address is also PII under HIPPA. An IP address is a number that identifies the address of a device connected to the Internet. *Id*. at 146.

Plaintiff asserts that Salem Health was compensated for this data and the data was used by Facebook and Google to optimize advertisements targeted to their users. *Id.* at 55-56, 164-167, 257.

In its motion to dismiss, Defendant asserts that Plaintiff consented to the disclosure of information via the Website's Terms of Service, and by creating Facebook and Google accounts, which requires agreeing to Facebook and Google's Terms of Service. MTD at 11; *see also* ECF No. 10 (Defendant's request for judicial notice of Facebook and Google's terms of service.)[2] Plaintiff alleges that she had no knowledge of Defendant's Tracking Tools and would not have consented to the disclosure of their information to third parties. Compl. ¶ 15, 59-60, 226.

II. HPPA Standards

Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization. *See* Health Insurance Portability and Accountability Act

[2] Federal Rule of Evidence 201(b) allows the Court to "judicially notice a fact that is not subject to reasonable dispute [if] it . . . can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." In addition, under the "incorporation by reference" doctrine, the Court may consider "the existence and contents" of documents relied upon or referenced by plaintiffs in their complaint. *Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005); *In re NVIDIA Corp. Sec. Litig*., 768 F.3d 1046, 1058 n. 10 (9th Cir. 2014)

("HIPPA"), 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i). The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."

The Privacy Rule broadly defines "protected health information" ("PHI") as individually identifiable health information ("IIHI") that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103. 121. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider, health plan, employer, or health care clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

Under the HIPPA de-identification rule, "health information is not individually identifiable only if": (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a

subject of the information" and "documents the methods and results of the analysis that justify such determination'"; or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed[:]

> a. Names;
>
> * * *
>
> H. Medical record numbers;
>
> * * *
>
> J. Account numbers;
>
> * * *
>
> M. Device identifiers and serial numbers;
>
> N. Web Universal Resource Locators (URLs);
>
> O. Internet Protocol (IP) address numbers; … and
>
> R. Any other unique identifying number, characteristic, or code…"
>
> * * *
>
> "The covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."

45 C.F.R. § 160.514.

An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 ("Part C"): "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual." The statute states that a "person … shall be considered to have obtained or disclosed individually

identifiable health information in violation of [Part C] if the information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320d-6.

III. Protected Health Information Under Oregon Law

Oregon law provides that "(1) It is the policy of the State of Oregon that an individual has:(a) The right to have protected health information of the individual safeguarded from unlawful use or disclosure." ORS § 192.553. Oregon law also provides in ORS § 192.558 that PHI may only be used or disclosed consistent with prior authorization or without such authorization in particular circumstances.

LEGAL STANDARD

To survive a motion to dismiss under the federal pleading standards, a pleading must contain a short and plain statement of the claim and allege "sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 667 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). While a pleading does not require "detailed factual allegations," it needs more than "a formulaic recitation of the elements of a cause of action." *Iqbal*, 556 U.S. at 677-78. "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. The plausibility standard . . . asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* at 678. Legal conclusions without any supporting factual allegations do not need to be accepted as

true. *Id.*

DISCUSSION

Plaintiff brings claims for (1) breach of confidence; (2) unauthorized interception, use and disclosure in violation of the Electronic Communications Privacy Act ("ECPA"); (3) intrusion upon seclusion; (4) breach of implied contract; (5) unjust enrichment; and (6) negligence.

Defendant argues that the second claim under the ECPA should be dismissed because Plaintiff has not pled an unauthorized interception and, regardless, as a party, Defendant could consent to any interception. Defendant contends that the third claim for intrusion upon seclusion should be dismissed because no intentional intrusion occurred, and no intrusion occurred that would be highly offensive to a reasonable person. Defendant argues the fourth claim for breach of implied contract should be dismissed because Plaintiff cannot show the existence of mutual assent or consideration. Defendant argues the fifth claim for unjust enrichment fails because it is not a cause of action in Oregon and Plaintiff has another remedy available. Defendant argues that the sixth claim for negligence is barred by the economic loss rule and Plaintiff did not properly allege damages.

I. Count One: Breach of Confidence

Defendant moves to dismiss Plaintiff's claim for breach of confidence on the basis that the disclosed information was not protected medical information, and that Plaintiff consented to the disclosure. MTD at 18.

To state a claim for beach of confidence, a plaintiff must allege an "unauthorized and unprivileged disclosure of confidential information obtained in a

confidential relationship." *Humphers v. First Interstate Bank of Or.*, 298 Or. 706, 717 (1985). The basis for this confidential relationship must be "determined by a legal source external to the tort claim itself." *A. B. v. Or. Clinic*, 321 Or. App. 60, 70 (2022) (quoting *Humphers*, 298 Or. at 718). The burden is on the plaintiff to identify this source and show that it creates a duty to keep the information at issue confidential. *Id.*

Here, Plaintiff claims that HIPAA, ORS §§ 192.553 to 192.581 (governing protected health information ("PHI"), and the "implied covenant of trust and confidence" inherent in a physician-patient relationship creates a duty of to keep protected health information confidential. Compl. ¶¶ 186–87.

Defendant contends that the information disclosed could not plausibly fit the statutory definition of protected health information. HIPAA (45 CFR § 160.103) and ORS § 192.556 define PHI similarly as information "created or received by a health care provider . . . and [r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care." 45 CFR § 160.103.

Plaintiff alleges that Defendant's Tracking Tools sent the following information to third parties:

> (1) status as medical patients; (2) health conditions; (3) desired medical treatment or therapies; (4) desired locations or facilities where treatment was sought; (5) phrases and search queries (such as searches for symptoms, treatment options, or types of providers); and (6) searched and selected physicians and their specialties conducted via the general search bar.

Compl ¶ 61.

Plaintiff has plausibly pled violations of HIPAA privacy requirements. *See, e.g*. Compl. ¶¶ 88-90 (image showing that tracking tools on Defendant's Website reveal name of financial assistance form to Google, thereby revealing the user's status as a patient and that the patient is seeking financial assistance). As noted in the Complaint, HHS has expressly stated that entities like Defendant that implement the Facebook Pixel and Google Analytics and disclose patient information have violated HIPAA Rules unless those entities obtain a HIPAA-complaint authorization. Compl. ¶ 29. No such authorization was obtained. Thus, Plaintiff's claim that Defendant has violated HIPAA's confidentiality requirements is at least plausible at this stage of litigation. Defendant's motion to dismiss is denied as to this issue.

II. Electronic Communications Privacy Act ("ECPA")

Defendant argues that the second claim under the ECPA should be dismissed because Plaintiff has not pled an unauthorized interception and, regardless, as a party, Defendant could consent to any interception. MTD at 16-19.

In 1986, Congress passed a law called the Electronic Communications Privacy Act ("ECPA") to protect the privacy of electronic communications. Pub.L. No. 99–508, 100 Stat. 1848. Title I of the ECPA amended the Wiretap Act to expand its coverage beyond wire and oral communication and "address[ ] the interception of . . . electronic communications." S.Rep. No. 99–541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557. Title II of the ECPA created the Stored Communications Act, which was created to "address[ ] access to stored wire and electronic communications and transactional records." *Id.*

The ECPA "provides a private right of action against any person who 'intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.'" Rodriguez v. Google LLC, No. 20-cv04688-RS, 2021 WL 2026726, at *6 (N.D. Cal. 2021). In *Campbell v. Facebook Inc.*, the Court explained:

> As the statutory text indicates, the focus of this provision is on the interception of the communication itself. While another provision of the Wiretap Act prohibits the use of the contents of a communication, that prohibition applies only if the interception itself is unlawful under section 2511(1)(a). Specifically, section 2511(1)(d) applies to any person who "intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication," but only if that person knows or has reason to know "that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection." See 18 U.S.C. § 2511(1)(d) (emphasis added). In other words, if there is no unlawful interception, there can be no unlawful use.
>
> 77 F. Supp. 3d 836, 840 (N.D. Cal. 2014) (emphasis added).

The statute defines "intercept" as "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." 18 U.S.C. § 2510(4). The 9th Circuit has provided additional guidance on how to interpret this term. "To be 'intercepted' in violation of the Wiretap Act, [a communication] must be acquired during transmission, not while it is in electronic storage." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 878, (9th Cir. 2002).

Defendant maintains that an "interception" within the meaning of the statute did not occur because the Tracking Tools do not contemporaneously capture and transfer patient data to Meta and Google, but instead copy the patient's data and

transmit it over in a separate second transmission. MTD at 17. Some California courts have found that the function of similar tools does meet the definition of "interception" under the ECPA because an interception does not occur while the data is in transit. *See e.g. Barbour v. John Muir Health*, No. C22-01693, 2023 WL 2618967, at *5 (Cal. Super. Ct. 2023). However, at this stage, the Court reviews allegations in Plaintiff's complaint and does not weigh the evidence about the disputed method by which the Tracking Tools function.

In the Complaint, Plaintiff states that "Defendant has effectively used its source code to commandeer and 'bug' or 'tap' its patients' computing devices, allowing Facebook, Google, and other third parties to listen in on all of their communications with Defendant and thereby intercept those communications." Compl. ¶ 55. Further, that the Tracking Tools "manipulate[] the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) with Defendant and to send those communications to Facebook and Google. These transmissions occur contemporaneously." *Id.* ¶ 56. Accepting as true allegations that Tracking Tools function as Plaintiff asserts, this would plausibly meet the definition of an "interception" under the statute.

Defendant argues that Plaintiff's consent to the disclosure of any information bars the Plaintiff's claim under the ECPA. The ECPA states that "[i]t shall not be unlawful" to intercept a communication "where one of the parties to the communication has given prior consent to such interception." 18 U.S.C. §2511(2)(d). However, § 2511(2)(d) describes a crime/tort exception, which clarifies that a "party

to the communication" may be liable where a "communication is intercepted for the purpose of committing any criminal or tortious act." *Id.*

The Court finds that Plaintiff has plausibly pled the crime/tort exception and, thus, Defendant cannot defeat Plaintiff's claim by consenting to the interception of the PHI. At this stage in the litigation, Plaintiff's claim sufficiently alleges a violation under the ECPA.

III. Intrusion Upon Seclusion

To state a claim for invasion of privacy, a Plaintiff must show "(1) an intentional intrusion, physical or otherwise, (2) upon the plaintiff's solitude or seclusion or private affairs or concerns, (3) which would be highly offensive." *Reed v. Toyota Motor Credit Corp.*, 301 Or App 825, 830-31, 459 P3d 253, 257 (2020), citing *Mauri v. Smith*, 324 Or. 476, 482, 929 P.2d 307 (1996). Defendant contends that Plaintiff has failed to allege an intentional intrusion and any alleged intrusion was not highly offensive.

Defendant argues that no intentional intrusion occurred because patients, like Plaintiff, voluntarily disclosed their information to Salem Health. Generally, if a party is aware of an observer's presence and still voluntarily chooses to disclose information, no intentional intrusion occurs. *See Snipes v. Wilkie*, No. 18-cv-03259-TSH, 2019 WL 1283936, at *7 (N.D. Cal. 2019).

Here, Plaintiff alleges that she was unaware that her information was being sent to third parties and that she could not make an informed choice to disclose information to unknown parties. Plaintiff alleges that she voluntarily disclosed PHI

to Defendant as a part of the patient-physician relationship, but never intended Google and Facebook to receive it. Therefore, Plaintiff has plausibly alleged an intentional intrusion.

Defendant argues that any alleged intrusion that occurred was not highly offensive because Plaintiff had no reasonable expectation of privacy and Salem Health did not have improper motives for the alleged disclosures. Defendant is correct that there is not a reasonable expectation of privacy in some standard internet activity, such as web searches. *See e.g. United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007); *People v. Nakai*, 183 Cal. App. 4th 499, 518 (2010).

Congress and courts have consistently noted that personal medical information is among the most sensitive information that could be collected about a person, and the existence of many statutes like HIPAA and ORS § 192.553 regulating its disclosure supports this idea. *See Perez-Denison v. Kaiser Found. Health Plan of the Nw.*, 868 F. Supp. 2d 1065, 1090 (D. Or. 2012) ("HIPAA suggests Congress has determined reasonable people want their medical records private and strongly object to those records being inappropriately accessed). It is likely that disclosure of such personal and sensitive information would be highly offensive to a reasonable person. Therefore, Plaintiff has pled a valid claim for intrusion upon seclusion.

IV. Breach of Implied Contract

Plaintiff asserts a claim for breach of an implied contract between the parties. "An implied-in-fact contract, like any other contract, must be founded upon the mutual agreement and intention of the parties." *Moyer v. Columbia State Bank*, 315

Or. App. 728, 737 (2021) (internal quotation marks omitted). "A contract does not arise because one party desires it; there must be *mutual* assent. As we said in *Ken Hood Construction*, 'Contract formation requires "a bargain in which there is a manifestation of mutual assent to the exchange and a consideration." *Restatement (Second) of Contracts* § 17(1) (1981).'" *Moyer v. Columbia State Bank*, 315 Or. App. 728, 737, 503 P.3d 472, 477 (2021) (quoting *Ken Hood Construction v. Pacific Coast Construction*, 201 Or. App. 568, 577, 120 P.3d 6 (2005)). "Unlike an express contract where an agreement is formed based on words, in an implied contract, the parties' agreement is inferred, in whole or in part, from their conduct." *Id.* at 737–38; *see also Gadalean v. SAIF*, 364 Or. 707, 717 n.3 (2019) ("This court has explained that a contract implied in fact arises where the natural and just interpretation of the acts of the parties warrants such [a] conclusion.").

Plaintiff claims there was an implied contract between patients and Salem Health that was breached by Salem Health when they disclosed patient information to third parties. The Court finds Plaintiff's allegations insufficient to state a claim. Plaintiff has not pled facts tending to show that a meeting of the minds existed between this parties. When patients come to Salem Health Hospital seeking treatment, they enter a contract in which patients agree to pay for medical services and Defendant agrees to provide them. Patients understand that they are entering into a physician-patient relationship and can expect that Defendant will act in accordance with laws like HIPAA. However, Plaintiff has not pled facts that show Defendant's prospective patients would understand that they were entering into a

contract to keep their information confidential. Entering into an implied contract requires "mutual agreement and intent" of both parties. A patient's choice to use Defendant as a medical service provider does not indicate an intention to enter into an implied contract for the security of information entered on Defendant's website. Although the parties undoubtedly agreed to enter into a contract for medical services, Plaintiff has failed to show that patients could plausibly believe that an implied contract existed to keep information entered on Defendant's website confidential. Defendant's motion is granted as to this claim.

IV. Unjust Enrichment

The plaintiff asserts a claim for unjust enrichment on that basis that Plaintiff and class members provided Defendant with their confidential information and Defendant unjustly retained the benefit from the sale of this information. Defendant first argues in their motion to dismiss that unjust enrichment is not an independent cause of action in Oregon.

The Oregon Supreme Court recently discussed unjust enrichment claims under Oregon law in *Larisa's Home Care, LLC v. Nichols-Shields*, 362 Or. 115, 404 P.3d 912 (2017). The court explained that "Oregon courts should examine the established legal categories of unjust enrichment as reflected in Oregon case law and other authorities to determine whether any particular enrichment is unjust." *Id.* at 132. When applying this doctrine, Oregon courts must determine whether the alleged enrichment is unjust by examining whether the allegations match already recognized forms of unjust enrichment by Oregon case law and treatises.

In this case, Plaintiff clarified in their Response that they intended to plead a quasi-contractual claim of unjust enrichment. Resp. at 29. Oregon courts have recognized this type of unjust enrichment claim. *See* e.g. *Farmer v. Groves*, 276 Or. 563, 568, 555 P.2d 1252 (1976); *Wilson v. Gutierrez*, 261 Or. App. 410, 414–15, 323 P.3d 974, 978 (2014). The elements for this claim are "(1) a benefit conferred, (2) awareness by the recipient that she has received the benefit, and (3) it would be unjust to allow the recipient to retain the benefit without requiring her to pay for it." *Cron v. Zimmer*, 255 Or. App. 114, 130, 296 P.3d 567 (2013). The Complaint alleges that the benefit conferred was medical information of patients; that Defendant took affirmative steps to collect it; and that it would be unjust for Defendant to retain the benefit from selling this information to advertisers. This amounts to a plausible claim for unjust enrichment.

Defendant also contends that since Plaintiff has an adequate remedy at law the unjust enrichment claim must be dismissed. At this stage of the proceedings, it would not be appropriate to dismiss this claim for that reason. *See Martell v. Gen. Motors LLC*, 492 F. Supp. 3d 1131, 1148 (D. Or. 2020) (denying motion to dismiss unjust enrichment claim and stating, "[a]t this stage of the litigation, it is unknown whether the remedy at law meets this standard."). Defendant's motion is denied on this issue.

V. Negligence

To prove a negligence claim, one "must allege facts from which a factfinder could determine (1) that defendant's conduct caused a foreseeable risk of harm, (2)

that the risk is to an interest of the kind that the law protects against [], (3) that [the] defendant's conduct was unreasonable in light of the risk, (4) that the conduct was a cause of plaintiff's harm, and (5) that [the] plaintiff was within the class of persons and plaintiff's injury was within the general type of potential incidents and injuries that made defendant's conduct negligent." *Tomlinson v. Metro. Pediatrics, LLC*, 275 Or. App. 658, 676 (2015), *aff'd*, 362 Or. 431 (2018).

Defendant alleges that (1) Plaintiff's negligence claim is barred by the economic loss doctrine, and (2) Plaintiff fails to allege recoverable damages. MTD at 26.

As damages, Plaintiff has pled a loss of privacy. Compl. ¶ 229-e. Courts have recognized loss of privacy constitutes damages for a negligence claim. See, e.g., Mehta v. Robinhood Fin. LLC, No. 21-CV-01013-SVK, 2021 WL 6882377, at *6 (N.D. Cal. May 6, 2021) ("As to damages, Plaintiffs adequately allege damages, including 'the loss of control over the use of their identity, harm to their constitutional right to privacy, … and privacy injuries associated with having their sensitive personal and financial information disclosed.'") (citation omitted); Flores-Mendez v. Zoosk, Inc., No. C 20- 04929 WHA, 2021 WL 308543, at *4 (N.D. Cal. Jan. 30, 2021) ("[P]laintiffs adequately allege damages in the form of … loss of privacy with respect to highly sensitive information … and risk of embarrassment."). This is particularly true in the pixel context. *See, e.g., In re Grp. Health Plan Litig*., 2023 WL 8850243, at *6 ("Plaintiffs have alleged loss of privacy, mental anguish, diminished value of private information, and other forms of harm. The forms of damages sought by Plaintiffs are

cognizable.") (internal citation omitted). Plaintiff has satisfied the damages element for a common law claim of negligence, and her claim is not precluded by the economic loss doctrine.

Plaintiff has also alleged as damages the diminished value of their private information. Compl. ¶ 196-h. Courts in the Ninth Circuit and around the country have accordingly held that the diminished value of sensitive health or personal information supports a negligence claim. *See, e.g., Brown v. Google, LLC*, 2021 WL 6064009, at *17 (N.D. Cal. Dec. 22, 2021) ("*Brown I*") (plaintiffs lost money when Google took "valuable data" and "received no money in return"); *Calhoun v. Google LLC*, 526 F.Supp.3d 605, 635 (N.D. Cal. 2021); *Feins v. Goldwater Bank NA*, 2022 WL 17552440, at *8 (D. Ariz. Dec. 9, 2022) (recognizing diminished value of PII); *In re Marriott Int'l, Inc., Cust. Data Sec. Breach Litig*., 440 F. Supp. 3d 447, 461 (D. Md. 2020) ("[T]he growing trend across courts that have considered this issue is to recognize the lost property value of this information.").

At this stage of litigation, Plaintiff has plausibly alleged damages under their negligence claim. Defendant's motion is denied as to this claim.

B. Economic Loss Doctrine.

Alternatively, Defendant argues that Plaintiff's negligence claim is barred by the Economic Loss Doctrine. Plaintiff alleges that Defendant had a duty to keep its patients' Private Information confidential under ORS § 192.553. Defendant contends that the economic loss rule prohibits Plaintiff from raising a negligence claim on the basis that Plaintiff's loss is purely economic. MTD. at 26, *citing Harris v. Suniga*,

344 Or. 301, 305 (2008). However, the economic loss doctrine only "bars a party that has suffered a purely economic loss from bringing a negligence action," and regardless, does not apply if "there is a special relationship between the parties." *Harris v. Suniga*, 344 Or. 301 at 305 (emphasis added). "Examples of special relationships include lawyer-client relationships, physician-patient relationships and trustee-beneficiary relationships." *Doe v. Wright*, No. 2:23-CV-00332-HL, 2023 WL 6810734, at *17 (D. Or. Oct. 16, 2023). Defendant's motion to dismiss is denied as to this issue.

CONCLUSION

For the reasons set forth above, Defendants' Motion to Dismiss, ECF No. 9, is DENIED IN PART and GRANTED IN PART. Count IV of the Complaint is DISMISSED.

It is so ORDERED and DATED this 28th day of August 2024.

/s/Ann Aiken
ANN AIKEN
United States District Judge