

**UNITED STATES DISTRICT COURT  
DISTRICT OF MINNESOTA**

In re: CHANGE HEALTHCARE, INC.  
CUSTOMER DATA SECURITY  
BREACH LITIGATION

MDL No. 24-3108 (DWF/DJF)

This Document Relates to All Individual  
Patient Actions

**MEMORANDUM  
OPINION AND ORDER**

**INTRODUCTION**

This matter is before the Court on Defendants'<sup>1</sup> motion to dismiss (Doc. No. 256) the master complaint filed by Individual Plaintiffs<sup>2</sup> (Doc. No. 406 (“Compl.”)).<sup>3</sup>

---

<sup>1</sup> “Defendants” refers to: UnitedHealth Group Incorporated (“UHG”); Optum, Inc. (“Optum”); Optum Insight, Inc. (“Optum Insight”); and Change Healthcare, Inc. (“Change Healthcare”). (Compl. at 7.)

<sup>2</sup> “Individual Plaintiffs” refers to: Amanda Christenson; Taisha Dixon; Tracy Anne Phillips; Paul Avery; Jacqueline Jackson; Robin Dugan; Tawfik Mammad; Zoe Madonna; Kali Warren; Bethany Conley; Brittany Meadows; Olga Diatlova; Lashanden Darby; Edith Antonio; Amanda Rape; Deana Leffers; M.O.; Joshua Lowe; Rene Sims; Hailey Kleinheksel; Michelle Carter; Marissa Hatfield; Cedric Bonier; Jan Merrill; Richard Seibert; Michael Paul; DeBorah Evans; Lisa Brooks; David Powers; Roxanne Allen; Patricia Baggett; Kenya Jones; Edwin Hoag; Richard Schwalbe; Delmar Kentner; Dawn Duncan; Rosa Rubera; Matthew Loforese; Carol Slack; Rachael Schiller; Tristano Korlou; Patricia Donadio; James Morgan; Kaela Poitra; Autumn Abramczyk; Anna Griffith; Preslee Thorne; Robin Lanier; Ashley Harbon; Kim Kaehler; Sally Kirkpatrick; Tess Bussick; Lori Tynch; Polly Rush; Anna Lovell; Christina Estep; Alfred Williams, Sr.; Angela Johnson; Trudy Agres; Leigh Thompson (Tom) Hanes; J’Andre Ivory; Harry Knopp; Mark Wetzel; Luke Anderson; and Lauren Fossen. (Compl. ¶¶ 17-147.)

<sup>3</sup> The motion was originally filed to dismiss the consolidated class action complaint in *Christenson et al. v. UnitedHealth Group Inc. et al.*, No. 25-cv-183. The Court directed Plaintiffs to file the complaint directly onto the docket for this multi-district litigation (“MDL”). (See Doc. No. 403.)

Individual Plaintiffs oppose the motion. (Doc. No. 329.) For the reasons set forth below, the Court grants in part and denies in part the motion.

## **BACKGROUND**

This MDL stems from a cyberattack on Change Healthcare’s network and the resulting data breach. Individual patients and healthcare providers from across the country sued Change Healthcare and various parent and partner organizations. Those cases were then consolidated in the District of Minnesota for pretrial purposes by the Judicial Panel on Multidistrict Litigation. (Doc. No. 1.)

### **I. The Change Healthcare Platform**

Change Healthcare is a healthcare data company. (Compl. ¶ 157.) Change Healthcare operates a platform through which healthcare providers and payers communicate regarding healthcare service claims, and which facilitates data transfers between healthcare providers and insurers for purposes of both clinical decision-making and payment processing (the “Platform”). (*Id.* ¶ 158.) That data exchange occurs through an Electronic Data Interchange (“EDI”) clearinghouse. (*Id.* ¶¶ 158-63.) The Platform is the largest clearinghouse in the United States. (*Id.* ¶ 165.) The Platform processes approximately 15 billion healthcare transactions annually, representing over half of medical claims in the country and totaling approximately \$1.5 trillion<sup>4</sup> in medical claims. (*Id.* ¶¶ 2, 165.)

---

<sup>4</sup> The Provider Plaintiffs’ complaint states that the Platform processes approximately \$2 trillion in medical claims. (Doc. No. 407 ¶ 1.) This discrepancy is not important to the resolution of the pending motion.

This work requires Change Healthcare to collect vast amounts of data, including personally identifiable information (“PII”) and protected health information (“PHI”), collectively, “Personal Information.” “Data that is typically entered into the Change Platform include full names, phone numbers, addresses, Social Security numbers, dates of birth, email addresses, medical records, specific treatment information, dental records, payment information, claims information, and insurance records.” (*Id.* ¶ 178.)

## II. The Cyberattack

On February 12, 2024, cybercriminals breached Change Healthcare’s network (the “Cyberattack”). (*Id.* ¶¶ 1, 251.) The Cyberattack was orchestrated by a ransomware group called ALPHV, a group notorious for targeting healthcare entities. (*Id.* ¶¶ 6, 232, 237-44.)

First, ALPHV used the user credentials of a low-level employee, found in a group chat that advertises the sale of stolen credentials to cybercriminals,<sup>5</sup> to access a remote portal of Change Healthcare’s network. (*Id.* ¶¶ 7, 251.) Once in the network, the cybercriminals created privileged accounts with administrator capabilities. (*Id.* ¶ 254.) They then used those administrator accounts to install malware tools and “backdoors” to ensure continued access to the network if Change Healthcare discovered their activity and attempted to block access. (*Id.* ¶ 255.)

---

<sup>5</sup> It is unclear how the credentials were obtained and added to that group chat. (Compl. ¶ 252.)

While in the network, ALPHV exfiltrated data (the “Data Breach”). (*Id.* ¶ 274.) The data stolen was the Personal Information of over 190 million<sup>6</sup> patients. (*Id.* ¶ 1.) This data included military personnel PII; medical records; dental records; payment information; claims information; patient PII such as phone numbers, emails, addresses, and Social Security numbers; source code files; and insurance records. (*Id.* ¶ 260.) This constitutes the largest healthcare data breach in the United States. (*Id.* ¶ 1.) ALPHV then posted the exfiltrated data on the dark web. (*Id.* ¶ 276.)

On February 21, 2024, nine days after the initial access, ALPHV deployed ransomware which blocked Defendants’ access to Change Healthcare’s networks. (*Id.* ¶¶ 256-57, 274.) Defendants did not discover ALPHV’s activity until this deployment. (*Id.* ¶ 256.) Upon learning of the Cyberattack, Defendants isolated the impacted systems and then shutdown the Platform’s operation. (*Id.* ¶¶ 258, 274, 356.)

To regain control of Change Healthcare’s systems and decrypt the stolen data, ALPHV demanded a \$22 million ransom from UHG, which UHG paid. (*Id.* ¶¶ 11, 277.) Individual Plaintiffs allege that this ransom payment was ineffective because ALPHV did not destroy the data and that ALPHV’s affiliate retains the data. (*Id.* ¶¶ 12, 279-82.)

---

<sup>6</sup> The complaint alleges that the data of over 120 million patients was exfiltrated. (Compl. ¶ 1; *see also id.* ¶ 275 (explaining impact and citing website where numbers are regularly updated).) Defendants’ most recent estimate is that approximately 192.7 million individuals were impacted. *Change Healthcare Cybersecurity Incident Frequently Asked Questions*, U.S. Dep’t of Health & Hum. Servs. (Mar. 14, 2025), <https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html>. The Court properly considers this update because it is embraced by the complaint. *See Porous Media Corp. v. Pall Corp.*, 186 F.3d 1077, 1079 (8th Cir. 1999).

Indeed, a ransomware group has confirmed that it possesses four terabytes of the stolen data, posted screenshots of that data on the dark web, and has attempted to extort more money from Defendants. (*Id.* ¶¶ 282, 291.) UHG CEO Andrew Witty testified that, despite the ransom payment, he could not guarantee that ALPHV or others did not retain copies of the data. (*Id.* ¶ 278.)

### **III. Security Measures**

Individual Plaintiffs allege that the Cyberattack was the result of deficient security measures on Change Healthcare’s network. (*Id.* ¶¶ 8, 14, 358.)

First, the portal to Change Healthcare’s network did not use multi-factor authentication (“MFA”). (*Id.* ¶¶ 8, 214, 272.) MFA is an identity verification method which requires at least two pieces of information to gain access. (*Id.* ¶¶ 214-15.) MFA is an effective way to prevent cyberattacks and widely recommended by experts. (*Id.* ¶¶ 220-22, 376-77.) Further, the failure to implement MFA was a violation of Change Healthcare’s policies. (*Id.* ¶ 273.) Due to the lack of MFA, ALPHV was able to more easily access the portal. (*Id.* ¶¶ 223, 253.) Indeed, ALPHV’s typical hacking tactics begin with “obtaining login credentials and exploiting systems that do not have MFA.” (*Id.* ¶ 249.) Witty admitted that the lack of MFA allowed ALPHV to access the network. (*Id.* ¶ 261.)

Second, the data stored by Change Healthcare was not encrypted. (*Id.* ¶¶ 9, 384, 405.) Multiple federal agencies recommend encrypting Personal Information to protect data even after a breach. (*Id.* ¶¶ 363, 383.) The network’s lack of encryption made it easier for ALPHV to view the data it exfiltrated. (*See id.* ¶ 384.)

Third, the system did not implement sufficient internal monitoring. (*Id.* ¶¶ 10, 224, 382.) Internal monitoring includes analyzing network usage to flag suspicious activity and identify system vulnerabilities. (*Id.* ¶¶ 225-26.) Cybersecurity experts, the Federal Trade Commission (“FTC”), and the Health Insurance Portability and Accountability Act (“HIPAA”) encourage internal monitoring. (*Id.* ¶¶ 352, 364, 379.) This lack of sufficient internal monitoring is allegedly the reason that ALPHV was in the system for nine days undetected. (*Id.* ¶ 227.) ALPHV installed software, ran administrator-only commands, and exfiltrated terabytes of data—all actions that should have been flagged by a monitoring system but were not. (*Id.* ¶¶ 228-29.)

Fourth, Change Healthcare did not segment its systems. (*Id.* ¶¶ 9, 354-56.) Data segmenting is the process of creating silos of data and software to prevent lateral movement within a system and protect the other silos if one silo is breached. (*See id.* ¶ 355.) Cybersecurity guidance encourages such segmentation. (*Id.* ¶ 357.) Segmenting systems could have prevented ALPHV from accessing other areas of the network from the original access point. (*See id.* ¶¶ 354-56.)

Fifth, the network did not limit employees’ access to the minimum necessary. (*Id.* ¶ 374.) Minimum necessary access means that a user is only granted access to data and systems which are necessary for their job, and blocked from those which are not. (*See id.*) Federal law and industry standards require application of this principle. (*Id.* ¶ 373.) Had Change Healthcare implemented such a system, ALPHV would not have been able to use the low-level employee’s credentials to create an administrative profile. (*Id.* ¶¶ 374-75.)

Individual Plaintiffs allege that Defendants knew or should have known about the risks of having deficient cybersecurity because healthcare companies are particularly at risk of cyberattacks. (*Id.* ¶ 346; *see also id.* ¶¶ 218, 329-31 (detailing the risks to healthcare organizations).) There have been many notable cyberattacks at healthcare organizations in recent years. (*Id.* ¶¶ 334-35.) UHG knew of this risk, having experienced over 450,000 intrusion attempts each year. (*Id.* ¶¶ 270, 338-40.) Further, HIPAA security standards require organizations to protect against anticipated threats. (*Id.* ¶ 378.)

Recognizing this heightened risk, Defendants made statements about the security of their systems. UHG and Optum’s privacy policy claimed that they maintained “administrative, technical, and physical safeguards” to protect patient data. (*Id.* ¶¶ 201, 210.) Change Healthcare’s privacy policy claimed that it utilized “security measures designed to safeguard the data [it] process[es] against unauthorized access.” (*Id.* ¶¶ 203, 208.) And Change Healthcare’s Code of Conduct emphasized the company’s commitment to data security. (*Id.* ¶ 204.)

#### **IV. The Aftermath**

Victims of cyberattacks who have had their data stolen face risk of identity theft. (*Id.* ¶ 297; *see also id.* ¶ 318 (explaining that stolen information exposes the victim to phishing attacks, which can lead to identity theft).) Identity theft is a broad term which encompasses both fraud on existing accounts and fraudulent creation of new accounts. (*Id.* ¶ 299.) Stolen personal information can be used to make unauthorized charges, open fraudulent accounts, obtain fraudulent identification documents, or a litany of other

crimes. (*Id.* ¶¶ 300-01.) When, as here, PHI is involved, consequences can include falsified information in a patient’s medical record and fraudulent insurance claims. (*Id.* ¶¶ 314-15, 317.)

Resolving harms of identity theft can be an arduous and timely process. (*Id.* ¶¶ 298, 302; *see also id.* ¶ 311 (listing FTC’s recommended steps to respond to identity theft).) This is especially so when data stolen includes Social Security numbers because of their sensitive nature and the difficulty to replace. (*Id.* ¶¶ 303-04.) But even if a victim takes the necessary steps, they continue to be at risk. (*Id.* ¶ 322.)

## **V. The Class Action**

Each Individual Plaintiff was notified that their data was potentially stolen in the Data Breach.<sup>7</sup> (*Id.* ¶¶ 17-147.) Individual Plaintiffs subsequently filed this consolidated class action complaint on behalf of themselves and all others similarly situated. (*Id.* ¶ 16.) The putative class includes patients whose data was held by Change Healthcare and compromised in the Data Breach. (*Id.* ¶ 386.)

Individual Plaintiffs allege numerous harms from the Cyberattack and the subsequent Data Breach:

- (1) loss of privacy;
- (2) misappropriation of their identity, name and likeness;
- (3) fraud and identity theft from the misuse of their stolen Personal Information;
- (4) diminution in the value of their Personal

---

<sup>7</sup> Each Individual Plaintiff alleges that they received a letter from Defendants notifying them that the Data Breach “may have involved” their data, but no Individual Plaintiff attaches any such letter to the complaint. Plaintiff Jason Coletti from a discrete case within the MDL filed the notice letter he received. (Civ. No. 24-3681, Doc. No. 1, Ex. 1 (“Notice Letter”).) Because the notice letter is embraced by the complaint, the Court may properly consider the letter. *See Porous Media Corp.*, 186 F.3d at 1079.

Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

(*Id.* ¶ 15.) Based on those harms, they bring the following claims: negligence (Count I), negligence per se (Count II), third-party beneficiary breach of contract (Count III), unjust enrichment (Count IV), declaratory judgment (Count V), and violation of thirty-six state consumer protection laws (Counts VI-XLI).<sup>8</sup> (*Id.* ¶¶ 397-1031.)

---

<sup>8</sup> Violation of Alabama's Deceptive Trade Practices Act (Count VI), violation of Alaska's Unfair Trade Practices and Consumer Protection Act (Count VII), violation of Alaska's Protection of Personal Information Act (Count VIII), violation of the Arizona Consumer Fraud Act (Count IX), violation of California's Unfair Competition Law (Count X), violation of the California Customer Records Act (Count XI), violation of the California Confidentiality of Medical Information Act (Count XII), violation of the California Consumer Privacy Act of 2018 (Count XIII), violation of the Colorado Consumer Protection Act (Count XIV), violation of the Connecticut Unfair Trade Practices Act (Count XV), violation of Georgia's Identity Theft Protection Act (Count XVI), violation of the Hawaii Unfair or Deceptive Acts or Practices Law (Count XVII), violation of the Illinois Consumer Fraud and Deceptive Business Practices Act (Count XVIII), violation of the Louisiana Database Security Breach Notification Law (Count XIX), violation of the Louisiana Unfair Trade Practices Act (Count XX), violation of the Maine Unfair Trade Practices Act (Count XXI), violation of the Maryland Consumer Protection Act (Count XXII), violation of the Massachusetts Consumer Protection Act (Count XXIII), violation of the Minnesota Deceptive Trade Practices Act (Count XXIV), violation of the Minnesota Health Records Act (Count XXV), violation of the New Hampshire Consumer Protection Act (Count XXVI), violation of the New Hampshire Right to Privacy Statute (Count XXVII), violation of the New Jersey Consumer Fraud Act (Count XXVIII), violation of the New Mexico Unfair Practices Act (Count XXIX), violation of New York General Business Law § 349 (Count XXX), violation of the North Carolina Unfair and Deceptive Trade Practices Act (Count XXXI), violation of the North Carolina Identity Theft Protection Act (Count XXXII), violation of Oregon Revised Statute § 646.608 (Count XXXIII), violation of the Rhode Island Unfair Trade Practice and Consumer Protection Act (Count XXXIV), violation of the South Carolina Unfair

These claims are brought against Change Healthcare, UHG, Optum, and Optum Insight. (Compl. at 7.) Change Healthcare is incorporated in Delaware and has its principal place of business in Tennessee. (*Id.* ¶ 157.) UHG is a vertically integrated healthcare company comprised of United Healthcare and Optum. (*Id.* ¶ 148.) UHG oversaw and was responsible for Change Healthcare’s technology. (*Id.* ¶ 407.) UHG is incorporated in Delaware and headquartered in Minnesota. (*Id.*) Optum is a subsidiary of UHG which operates Optum Health, Optum Insight, and Optum Rx. (*Id.* ¶ 149.) Optum took responsibility for Change Healthcare’s data and promised to safeguard it. (*Id.* ¶ 406.) Optum is incorporated in Delaware and has its principal place of business in Minnesota. (*Id.*) Optum Insight is a data analytics and technology company. (*Id.* ¶ 151.) Like Change Healthcare, Optum Insight operated an EDI clearinghouse, processing 192 million claims annually. (*Id.* ¶ 189.) In October 2022, Optum Insight merged with Change Healthcare. (*Id.* ¶ 153.) Optum Insight is incorporated in Delaware and has its principal place of business in Minnesota. (*Id.* ¶ 150.)

## DISCUSSION

### I. Standing

Article III limits the federal judicial power to “Cases” and “Controversies.” U.S. Const. art. III, § 2. “For there to be a case or controversy under Article III, the plaintiff

---

Trade Practices Act (Count XXXV), violation of South Carolina Code § 39-1-90 (Count XXXVI), violation of the Vermont Consumer Fraud Act (Count XXXVII), violation of the Washington Consumer Protection Act (Count XXXVIII), violation of the Washington State Data Breach Notification Act (Count XXXIX), violation of Wisconsin Statute §§ 146.81-.84 (Count XL), and violation of the Wyoming Consumer Protection Act (Count XLI).

must have a personal stake in the case—in other words, standing.” *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423 (2021) (citation modified). “[T]o establish standing, a plaintiff must show (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief.” *Id.* Standing must be assessed individually for each plaintiff, each claim, and each type of relief sought. *Id.* at 431. Plaintiffs, as the ones invoking the Court’s jurisdiction, bear the burden of establishing standing, but need only state general allegations of injury, traceability, and redressability. *Id.* at 430-31; *In re SuperValu, Inc.*, 870 F.3d 763, 773 (8th Cir. 2017).

Defendants first challenge the injury in fact of Plaintiffs Agres, Antonio, Hanes, Johnson, Kentner, Lovell, Schwalbe, and Seibert, contending that those Plaintiffs allege “only purported injuries like receipt of spam calls and time spent researching the Cyberattack or monitoring related to the same.” (Doc. No. 266 at 21; *see* Compl. ¶¶ 43, 66, 84, 86, 126, 132, 134, 136.) Defendants next challenge the traceability of each Individual Plaintiff’s injury to the Cyberattack. (Doc. No. 266 at 28-31.)

#### **A. Injury in Fact**

“To establish injury in fact, a plaintiff must show that he or she suffered ‘an invasion of a legally protected interest’ that is ‘concrete and particularized’ and ‘actual or imminent, not conjectural or hypothetical.’” *Spokeo, Inc. v. Robins*, 578 U.S. 330, 339 (2016) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992)). Individual Plaintiffs seek injunctive, declaratory, and monetary relief. (Compl. ¶ 1032.)

## 1. Injunctive and Declaratory Relief

Individual Plaintiffs allege that their stolen data “will continue to be leaked and traded on the dark web, meaning [they] will remain at an increased risk of fraud and identity theft.” (*Id.* ¶ 320.) For purposes of injunctive relief, a risk of future harm will suffice to establish standing if the threatened injury is “certainly impending, or there is a substantial risk that the harm will occur.” *SuperValu*, 870 F.3d at 769 (citation modified). In the data breach context, the breach alone does not suffice—there must be some indication that the breach will cause future harm. *See id.* at 769-70.

The Eighth Circuit’s ruling in *SuperValu* is instructive. *Id.* There, customers of a grocery store alleged that their financial information was stolen in a cyberattack on the grocery store network. *Id.* at 766. The court addressed whether that theft created a substantial risk that the customer-plaintiffs would suffer future identity theft. *Id.* at 770. The court reasoned that because the information allegedly stolen was only credit card information, not any personally identifying information, the plaintiffs were not at risk of future fraud. *Id.* at 770-71. Here, the information allegedly stolen included full names, Social Security numbers, dates of birth, medical records, and payment information. (Compl. ¶¶ 1, 178.) Unlike in *SuperValu*, this information can be used for identity theft. *See In re Netgain Tech., LLC*, No. 21-cv-1210, 2022 WL 1810606, at \*5 (D. Minn. June 2, 2022) (distinguishing *SuperValu* because PII and PHI were stolen, and collecting cases holding that there is a substantial risk when PII and PHI are stolen).

Additionally, the intention of the breach is relevant. Data taken in a hack orchestrated by a cybercriminal group is at a higher risk of misuse than data exposed

inadvertently. *See, e.g., id.; Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 153 (3d Cir. 2022). This Cyberattack by ALPHV, an organized cybercriminal group, is high risk. (*See* Compl. ¶¶ 232-49 (explaining the sophistication of ALPHV).) Further, Individual Plaintiffs’ allegations that some of the stolen data has already been misused indicates that all stolen data is at risk of misuse. *See, e.g., Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 376 (1st Cir. 2023) (“That at least some information stolen in a data breach has already been misused also makes it likely that other portions of the stolen data will be similarly misused.”). While this past misuse is not imputed to Plaintiffs Agres, Antonio, Hanes, Johnson, Kentner, Lovell, Schwalbe, and Seibert, it is indication that bad actors have the data and a desire to use it.

Defendants contend that UHG’s ransom payment eliminates this risk of future harm. (Doc. No. 266 at 23.) The Court disagrees. First, the ransom payment does not guarantee that ALPHV surrendered and no longer possesses the data. (*See* Compl. ¶ 287.) Second, the information was on the dark web for about a week—neither UHG nor ALPHV can guarantee that the information was not copied or downloaded in that time. (*See id.* ¶¶ 276, 278.) Indeed, Individual Plaintiffs allege that another ransomware group, RansomHub, claims to have four terabytes of the stolen data and is selling that data on the dark web. (*Id.* ¶¶ 12, 280-83, 291.) Further, Individual Plaintiffs allege harm that postdates the ransom. (*E.g., id.* ¶ 17 (alleging unauthorized charges in April, July, and September 2024).) Accepting the allegations as true, the ransom payment did not stop the dissemination of Individual Plaintiffs’ information, so it does not negate the risk of future harm.

All Individual Plaintiffs, including Plaintiffs Agres, Antonio, Hanes, Johnson, Kentner, Lovell, Schwalbe, and Seibert, face substantial risk of future identity theft and have therefore established standing for injunctive relief.

## **2. Monetary Relief**

Mere risk of future harm is, however, insufficient to establish standing for monetary relief. A plaintiff may establish standing for monetary relief by showing either (1) present harm or (2) a risk of future harm that caused a separate concrete harm. *TransUnion*, 594 U.S. at 436. Individual Plaintiffs allege “significant” time and expense responding to the Cyberattack. (*Id.* ¶ 325.)

Mitigation costs qualify as concrete injuries sufficient for standing for purposes of monetary relief when there is a substantial risk of future harm. *E.g.*, *In re Pawn Am. Consumer Data Breach Litig.*, No. 21-cv-2554, 2022 WL 3159874, at \*4 (D. Minn. Aug. 8, 2022); *cf. SuperValu*, 870 F.3d at 771 (finding that mitigation harms were not cognizable injury because there was not a substantial risk of future identity theft). Each Individual Plaintiff alleges lost time, effort, and expense responding to the Cyberattack and attempting to prevent the risk of future harm from manifesting. (Compl. ¶¶ 15, 17-147.) Having found that each Individual Plaintiff faces a substantial risk of future identity theft, it follows that each Individual Plaintiff has a cognizable harm via mitigation efforts related to that potential identity theft. Individual Plaintiffs have therefore also established injury in fact for purposes of monetary relief.

## **B. Traceability**

Article III standing also requires “a causal connection between the injury and the conduct complained of.” *Lujan*, 504 U.S. at 560. In the data breach context, allegations of (1) deficient cybersecurity that (2) resulted in a hack (3) in which data was stolen and (4) there was subsequent harm are sufficient to allege traceability. *SuperValu*, 870 F.3d at 772.

The Individual Plaintiffs allege that (1) Change Healthcare failed to secure personal information on its network, (2) Change Healthcare suffered the Cyberattack, (3) Individual Plaintiffs’ personal information was stolen in the Data Breach, and (4) Individual Plaintiffs experienced subsequent identity theft or other harms. This is sufficient to establish traceability to this Cyberattack. *See Netgain*, 2022 WL 1810606, at \*6 (finding that similar allegations sufficiently pled traceability to that data breach). Despite the inclusion of the necessary elements, Defendants argue that traceability is defeated for myriad reasons. (Doc. No. 266 at 28-31.) The Court will take each in turn.

### **1. Other Data Breaches**

The reality that many other data breaches happen does not negate Individual Plaintiffs’ allegations that the harm arose from this Cyberattack specifically. *See Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 696 (7th Cir. 2015). Additionally, each Individual Plaintiff received a notice letter that their data was potentially impacted. When a plaintiff has received a breach notice letter, a court can reasonably infer that harms are traceable to the breach in question. *See Stallone v. Farmers Grp., Inc.*, No. 21-cv-1659, 2022 WL 10091489, at \*9 (D. Nev. Oct. 15, 2022). Further, each

Individual Plaintiff alleges that they are careful with their data and practice cybersecurity measures. These allegations suggest that the harm did not come from a different breach. *See Webb*, 72 F.4th at 374 (finding that allegations that plaintiff was “very careful about sharing her PII” created an inference that the harm could not be traced to another breach). The existence of other data breaches does not defeat traceability.

## 2. Predated and Non-Dated Harms

Timing of harm is relevant to traceability. *See, e.g., id.* (discussing temporal connection between a data breach and the harm which allegedly flowed from it). Defendants ask the Court to strike injuries that predated the Cyberattack and any harms for which Individual Plaintiffs did not specify a date. (Doc. No. 266 at 29.)

Logically, only harms that postdate a data breach can be traced to that breach. Conversely, any injury predating the Cyberattack is not traceable to Defendants. Only one Individual Plaintiff references an injury that explicitly predates the Cyberattack. (Compl. ¶ 92 (alleging that Plaintiff Loforese was notified that his personal information was on the dark web in January 2024, a month before the Cyberattack).) The Court therefore strikes this allegation. *See Fed. R. Civ. P. 12(f); Jordan v. Best Buy Co.*, No. 24-cv-1066, 2025 WL 580894, at \*6 (D. Minn. Feb. 21, 2025) (explaining that a court has liberal discretion to strike material under Rule 12(f), including portions of a pleading). But since Plaintiff Loforese also alleges injuries that postdate the Cyberattack, this discrepancy does not defeat his standing. (Compl. ¶ 92 (alleging unauthorized transactions throughout 2024).)

While some Individual Plaintiffs do not specify a date on which harm occurred, the allegations clearly suggest that they postdate the Cyberattack. For example, allegations that an Individual Plaintiff experienced an uptick in phishing attacks after the Cyberattack suggests that their personal information was released due to the breach. (*E.g., id.* ¶ 18.) Plaintiffs do not need to plead the specific date of injury when the general allegations establish a postdated harm. *See In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 60-61 (D.C. Cir. 2019).

### **3. Ransom Payment**

Relatedly, Defendants contend that the ransom payment eliminates any threat of harm so any purported harm that postdates the ransom is not traceable. (Doc. No. 266 at 29.) For the same reasons discussed above, the ransom payment does not defeat traceability for harms post-ransom payment. The ransom payment cannot guarantee that the data is safe, and Individual Plaintiffs allege continuing harm. The cases cited by Defendants are inapposite because there was no alleged harm or future risk of harm. *See Patterson v. Med. Rev. Inst. of Am., LLC*, No. 22-cv-413, 2022 WL 2267673, at \*3 (N.D. Cal. June 23, 2022) (dismissing complaint for failing to allege that data was viewed or misused, and because the data was allegedly returned); *In re Practicefirst Data Breach Litig.*, No. 21-cv-790, 2022 WL 354544, at \*5 (W.D.N.Y. Feb. 2, 2022) (dismissing complaint for failure to allege any attempted or actualized fraud), *report and recommendation adopted*, 2022 WL 3045319 (W.D.N.Y. Aug. 1, 2022). Harms postdating the ransom payment are still fairly traceable to the Data Breach.

#### 4. Data Matching

Finally, traceability of harms in a data breach case requires that the information allegedly misused matches the information allegedly stolen. *See In re Samsung Data Sec. Breach Litig.*, 761 F. Supp. 3d 781, 800-01 (D.N.J. 2025).

Defendants first contend that Individual Plaintiffs' financial information was not held by Change Healthcare, so any financial harm is not traceable to the Data Breach. (Doc. No. 266 at 30.) But that contention is in direct conflict with the Individual Plaintiffs' allegations that Change Healthcare held payment information, claims information, and insurance records on its network, and the data breach notice letters in which Change Healthcare acknowledged that financial data may have been accessed. (Compl. ¶ 178; Notice Letter.) It may be discovered that certain Individual Plaintiffs' financial information was not taken, but, for now, the Court must accept the allegations in the complaint as true.

Similarly, Defendants argue that allegations of access to accounts on other websites is not traceable because Change Healthcare did not have the information necessary to access those accounts. (Doc. No. 266 at 30-31.) While true that the network did not have, for example, Plaintiff Tynch's Amazon account login, it held enough personal information to access any account. (*See* Compl. ¶ 122.) Individual Plaintiffs explain that identity thieves utilize Personal Information as a gateway to different avenues of fraud—once a criminal has some information, they can use that to access additional information. (*Id.* ¶¶ 301, 304.) Because Individual Plaintiffs allege that a vast range of data was stolen, namely Social Security numbers, the Court is satisfied that

access to an unrelated account is fairly traceable to the Cyberattack. *See Sanchez v. Xavier Univ. of La.*, No. 23-cv-1269, 2024 WL 4251906, at \*5 (E.D. La. July 18, 2024) (accepting that allegations of Social Security number theft are sufficient for access to any number of accounts); *cf. Crowe v. Managed Care of N. Am. Inc.*, No. 23-cv-61065, 2024 WL 6863341, at \*4 (S.D. Fla. Aug. 16, 2024) (explaining that hackers can use exposed information to guess usernames and passwords to unrelated accounts). Individual Plaintiffs have met their burden to show traceability.

### **C. Redressability**

Although Defendants do not contest redressability, the Court finds that Individual Plaintiffs' injuries are redressable. Individual Plaintiffs explain how the requested relief will likely be redressed by connecting the dots between the alleged harm and the impact of the requested relief. First, Individual Plaintiffs allege that Defendants' data security remains deficient, which puts them at imminent risk of a future data breach. (*E.g.*, Compl. ¶ 453.) This is sufficient to support standing for injunctive and declaratory relief. *Cf. Pawn Am.*, 2022 WL 3159874, at \*3 (finding a lack of redressability when plaintiffs failed to allege imminence of a future breach). Second, Individual Plaintiffs allege unreimbursed fraudulent charges and other out-of-pocket costs. (*E.g.*, Compl. ¶ 62.) These are redressable monetary harms. *See Remijas*, 794 F.3d at 696-67 (discussing redressability of unreimbursed charges and mitigation costs). Individual Plaintiffs have established injury in fact, traceability, and redressability, so they have standing.<sup>9</sup>

---

<sup>9</sup> Although the injury and causation inquiry under Rule 12(b)(6) is similar to the Article III standing inquiry, the Rule 12(b)(6) inquiry is ultimately more stringent. *See*,

## II. Choice of Law

Having established standing, but before turning to substantive analysis of the claims, the Court addresses choice of law.<sup>10</sup> Generally, federal courts analyze choice of law under the forum state's laws. *Klaxon Co. v. Stentor Elec. Mfg. Co.*, 313 U.S. 487, 496 (1941). However, for MDLs, the choice-of-law framework of the forum in which the complaint was brought governs. *In re Bair Hugger Forced Air Warming Devices Prods. Liab. Litig.*, 999 F.3d 534, 538 (8th Cir. 2021). All Individual Plaintiffs filed originally in the District of Minnesota, so the Court uses Minnesota's choice-of-law framework.

Minnesota's choice-of-law framework is a three-step inquiry. The Court (1) decides if there is a conflict between the laws of the two potential forums, (2) decides whether both laws can be constitutionally applied, and (3) weighs five factors to determine which law is more appropriately applied. *Nodak Mut. Ins. Co. v. Am. Fam. Mut. Ins. Co.*, 604 N.W.2d 91, 93-94, 94 n.2 (Minn. 2000). This framework applies to both tort-law and contract-law claims.<sup>11</sup> *See Jepson v. Gen. Cas. Co. of Wis.*, 513 N.W.2d

---

*e.g.*, *SuperValu*, 870 F.3d at 773. Applying that higher bar, the Court finds that Individual Plaintiffs' allegations go beyond Article III and establish injury and causation for purposes of Rule 12(b)(6).

<sup>10</sup> Individual Plaintiffs believe a choice-of-law analysis is premature. (Doc. No. 331 at 3-4; Doc. No. 419 at 2-4.) The Court finds it has sufficient information to decide this issue. *See Pioneer Civ. Constr., LLC v. Ingevity Ark., LLC*, 659 F. Supp. 3d 977, 986 (W.D. Ark. 2023).

<sup>11</sup> The framework does not apply if there is a relevant choice-of-law provision. *C.H. Robinson Worldwide, Inc. v. Traffic Tech, Inc.*, 60 F.4th 1144, 1148 (8th Cir. 2023); *see also Combined Ins. Co. of Am. v. Bode*, 77 N.W.2d 533, 536 (Minn. 1956) (holding that contractual choice-of-law provisions are enforced in Minnesota).

467, 470 (Minn. 1994) (applying the framework to both contract and tort claims, and explaining the difference in application).

**A. Conflict**

“A conflict exists if the choice of one forum’s law over the other will determine the outcome of the case.” *Nodak*, 604 N.W.2d at 94. The parties agree there are material conflicts (Doc. No. 255 at 4; Doc. No. 331 at 5), so the Court moves to the next step in the framework. *See Am. Guarantee & Liab. Ins. Co. v. U.S. Fid. & Guar. Co.*, 668 F.3d 991, 996 n.3 (8th Cir. 2012) (accepting the parties’ agreement on a conflict as sufficient to continue the analysis under Missouri’s choice-of-law framework).

**B. Constitutionally Applied**

Because an actual conflict exists, the Court must ensure the laws of each potential state can be constitutionally applied. *Jepson*, 513 N.W.2d at 469. That is, “that state must have a significant contact or significant aggregation of contacts, creating state interests, such that choice of its law is neither arbitrary nor fundamentally unfair.” *Id.* (citation modified).

The Court finds that it can constitutionally apply the law of any state. Change Healthcare did business in each of the fifty states and D.C., creating significant contacts and state interest in each. (*See* Compl. ¶¶ 175-76 (discussing the ubiquity of Change Healthcare in the American healthcare system).) This is evidenced by at least one Individual Plaintiff from each state and D.C. Defendants could have expected litigation to occur in any location, so any substantive law can be constitutionally applied.

### C. Choice Influencing Factors

Third, the Court considers five “choice influencing factors” to determine which law should apply: “(1) predictability of result; (2) maintenance of interstate and international order; (3) simplification of the judicial task; (4) advancement of the forum’s governmental interest; and (5) application of the better rule of law.” *Jepson*, 513 N.W.2d at 470.

“Predictability of results applies primarily to consensual transactions where the parties desire advance notice of which state law will govern in future disputes.” *Myers v. Gov’t Emps. Ins. Co.*, 225 N.W.2d 238, 242 (Minn. 1974). “The objective of the predictability factor is to fulfill the parties’ justified expectations.” *Lommen v. City of East Grand Forks*, 522 N.W.2d 148, 150 (Minn. Ct. App. 1994). Because Minnesota is the principal place of business of three of the Defendants, it was predictable that Minnesota law would apply. *Cf. GreenState Credit Union v. Hy-Vee, Inc.*, 549 F. Supp. 3d 969, 978 (D. Minn. 2021) (“All of Hy-Vee’s relevant information security employees and decision-making are located in Iowa. It is predictable that Iowa law would apply.”). Similarly, because Change Healthcare processed data for patients nationwide, it was predictable that the home-state laws of potential plaintiffs would apply. *See In re Grand Theft Auto Video Game Consumer Litig.*, 251 F.R.D. 139, 152 (S.D.N.Y. 2008) (emphasizing that parties who deliberately enter into transactions have “every reason to expect” that the law of the place in which the transactions occurred would apply). This factor is neutral.

The maintenance-of-interstate-order factor concerns whether the application of one state’s law would manifest disrespect for another’s sovereignty or “impede the interstate movement of people and goods.” *Jepson*, 513 N.W.2d at 471. “[M]aintenance of interstate order is generally satisfied as long as the state whose laws are purportedly in conflict has sufficient contacts with and interest in the facts and issues being litigated.” *Myers*, 225 N.W.2d at 242. “The primary focus is on the contacts that each competing state has with the dispute.” *Perry ex rel. Sherrell v. Beltrami County*, 520 F. Supp. 3d 1115, 1123 (D. Minn. 2021). By conducting business from and within Minnesota, Defendants had significant contacts with the state. *Cf. GreenState*, 549 F. Supp. 3d at 978 (“The actions and omissions by Hy-Vee giving rise to GreenState’s claims—its data security decision-making and the actions of the information technology department—are based in Iowa.”). But the Individual Plaintiffs’ contact with their home states is stronger and by doing business with Plaintiffs, Defendants availed themselves of those laws. *Cf. Grand Theft Auto*, 251 F.R.D. at 152 (“[T]he application of Minnesota’s law—or the law of any state other than the state of purchase—to transactions that took place throughout the nation would constitute an unwarranted infringement upon other states’ sovereignty.”). This factor weighs in favor of applying each Individual Plaintiff’s home state’s laws.

The simplification-of-the-judicial-task factor “concerns the forum court’s ability to discern and apply the law of another state as compared to its own law.” *Lommen*, 522 N.W.2d at 152. This factor is neutral, as the Court is able to apply the law of any state. *See Hughes v. Wal-Mart Stores, Inc.*, 250 F.3d 618, 620 (8th Cir. 2001) (“A federal

district court is faced almost daily with the task of applying some state's law other than that of the forum state, and it is equally capable of resolving [a] dispute under [any state's] law.”).

The governmental-interest factor asks “which choice of law most advances a significant interest of the forum.” *Nodak*, 604 N.W.2d at 95 (quoting *Jepson*, 513 N.W.2d at 472). The Court considers the relative policy interests of the potential states. *GreenState*, 549 F. Supp. 3d at 978. While all states have an interest in protecting nonresidents harmed in that state, that interest is outweighed by other states' interests in protecting their residents. *See Hughes*, 250 F.3d at 621. Therefore, this factor usually weighs in favor of the state where the injury occurred. *In re Baycol Prods. Litig.*, 218 F.R.D. 197, 207 (D. Minn. 2003). This factor weighs in favor of applying the laws of each Individual Plaintiff's home state because that is where the injury occurred and those states have an interest in protecting their residents.

The fifth factor, the “better rule of law,” is given little weight and need not be considered when the choice-of-law question can be resolved using the other four factors. *Nesladek v. Ford Motor Co.*, 876 F. Supp. 1061, 1070 (D. Minn. 1994), *aff'd*, 46 F.3d 734 (8th Cir. 1995). Because the other factors weigh in favor of applying each Individual Plaintiff's home state's law, the Court will not consider which is the “better” rule of law.

In tort-law cases, the second and fourth factors are given greater weight. *See Perry*, 520 F. Supp. 3d at 1122-24; *Baycol*, 218 F.R.D. at 207. However, because Individual Plaintiffs allege negligence in decision-making, this is not a typical “accidental” tort case, and the first factor is still relevant. *GreenState*, 549 F. Supp. 3d

at 977-78. The first factor is neutral, but the second and fourth factors weigh in favor of applying each Individual Plaintiff's home state's law. Further, for tort claims, the place of injury is especially relevant. *See, e.g., Perry*, 520 F. Supp. 3d at 1123; *Baycol*, 218 F.R.D. at 207. Individual Plaintiffs were allegedly injured in their home states. The Court therefore holds that the law of each Individual Plaintiff's home state applies to their tort claims.

In contract-law cases, the first factor is given the greatest weight. *See Jepson*, 513 N.W.2d at 470. Because that factor is neutral, the Court looks to the other factors, which weigh in favor of applying each Individual Plaintiff's home state's law. The Court therefore holds that the law of each Individual Plaintiff's home state also applies to their contract claims.

However, the Court cannot decide the merits based on the law of each home state without complete briefing on the issues. Currently, the parties have only fully briefed Minnesota substantive law.<sup>12</sup> The Court therefore continues the substantive analysis for only the Minnesota-based Individual Plaintiffs.<sup>13</sup>

---

<sup>12</sup> Defendants submitted appendices summarizing the relevant laws for each home state in support of their motion to dismiss. (Doc. No. 267, Apps. A-F.) In opposition briefing, Individual Plaintiffs objected to Defendants' use of appendices. (*See* Doc. No. 329 at 64-65.) At the June 12, 2025 Status Conference, the Court overruled Plaintiffs' objections but noted that if the appendices were considered by the Court in its ruling, Plaintiffs would have the opportunity to file response appendices and Defendants would have the opportunity to reply. (*See* Doc. No. 396 at 8-9.)

Accordingly, the Court now orders response and reply briefing on the home-state laws for Plaintiffs Christenson, Dixon, Phillips, Avery, Jackson, Dugan, Mammad, Madonna, Warren, Conley, Meadows, Diatlova, Darby, Antonio, Rape, Leffers, M.O., Lowe, Sims, Kleinheksel, Carter, Hatfield, Bonier, Merrill, Seibert, Paul, Evans, Baggett,

### III. Failure to State a Claim

To survive a motion to dismiss, a complaint must contain “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). Although a complaint need not contain “detailed factual allegations,” it must contain facts with enough specificity “to raise a right to relief above the speculative level.” *Id.* at 555. “Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements,” will not pass muster under *Twombly*. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. at 555). In sum, this standard “calls for enough fact[s] to raise a reasonable expectation that discovery will reveal evidence of [the claim].” *Twombly*, 550 U.S. at 556. This is a more stringent standard than Article III standing. *Brown v. Medtronic, Inc.*, 628 F.3d 451, 459 (8th Cir. 2010).

#### A. Non-Change Defendants

As a final preliminary matter before diving into the merits of each claim, the Court must consider whether each Defendant is properly named in the complaint. Defendants argue that Individual Plaintiffs fail to state a claim against three of the four Defendants: UHG, Optum, and Optum Insight (the “Non-Change Defendants”). (Doc. No. 266 at 39.)

---

Jones, Hoag, Schwalbe, Kentner, Duncan, Rubera, Loforese, Slack, Schiller, Korlou, Donadio, Morgan, Poitra, Abramczyk, Griffith, Thorne, Lanier, Harbon, Kaehler, Kirkpatrick, Bussick, Tynch, Rush, Lovell, Estep, Williams, Johnson, Agres, Hanes, Ivory, Knopp, Wetzell, Anderson, and Fossen.

<sup>13</sup> Plaintiffs Brooks, Powers, and Allen bring claims of negligence (Count I), negligence per se (Count II), third party beneficiary breach of contract (Count III), unjust enrichment (Count IV), declaratory judgment (Count V), violation of the Minnesota Deceptive Trade Practices Act (Count XXIV), and violation of the Minnesota Health Records Act (Count XXV). The Court therefore addresses only these counts below.

Defendants first argue that the Non-Change Defendants did not owe a duty to the Individual Plaintiffs. While true that a parent corporation is not liable for the acts of its subsidiary, a parent company may be liable for its own actions. *See United States v. Bestfoods*, 524 U.S. 51, 61, 64-65, 64 n.10 (1998) (holding that when a facility is “so pervasively controlled by its parent,” the parent may be liable). Individual Plaintiffs sufficiently allege independent wrongdoing for each of the Defendants. The complaint alleges that Optum Insight collected data on behalf of Change Healthcare after the two entities merged, implicating a duty to safeguard for both entities, which was allegedly breached. (*See* Compl. ¶ 405.) The complaint next alleges that Optum promised to safeguard the data, thereby taking on the duty to safeguard. (*Id.* ¶ 406.) Finally, the complaint alleges that UHG was responsible for the cybersecurity measures of Change Healthcare, which were allegedly deficient. (*Id.* ¶ 407.) Change Healthcare was not a typical subsidiary of UHG—the control went much deeper than mere monitoring and supervision. *See Bestfoods*, 524 U.S. at 72 (explaining that mere monitoring of performance is insufficient to impose parental liability, and instead that parent liability depends on whether the parent’s actions “are eccentric under accepted norms of parental oversight”). Because each Defendant has allegedly accepted a duty to Individual Plaintiffs and allegedly breached that duty, each is a proper Defendant.

Next, Defendants argue that Individual Plaintiffs improperly grouped all Defendants together in their complaint. A complaint must allege “sufficient personal involvement” to survive a motion to dismiss. *Beck v. LaFleur*, 257 F.3d 764, 766 (8th Cir. 2001). A plaintiff must explain “who did what to whom” to provide fair notice to the

defendant of the grounds for a claim. *Tatone v. SunTrust Mortg., Inc.*, 857 F. Supp. 2d 821, 831 (D. Minn. 2012). “A complaint which lumps all defendants together,” despite the ability to explain each defendant’s role, fails to state a claim. *Id.*; *see also City of Wyoming v. Proctor & Gamble Co.*, 210 F. Supp. 3d 1137, 1153 (D. Minn. 2016) (differentiating between complaints which lack specificity due to “laziness or frivolity” and those which lack specificity due to a “practical difficulty” in identifying which defendant was responsible for what outcome). Because Individual Plaintiffs alleged that all Defendants took responsibility and were involved in cybersecurity decisions and other operations at Change Healthcare, the Court finds that making allegations against Defendants collectively was appropriate. Individual Plaintiffs cannot be expected to define the contours of the corporate relationship when Defendants have blurred the lines by splitting tasks and transferring duties across entities. This defeats Individual Plaintiffs’ ability to plead each Defendant’s role with specificity and the Court therefore holds that Plaintiffs sufficiently alleged personal involvement.

**B. Count I: Negligence<sup>14</sup>**

Minnesota follows the familiar negligence standard: a plaintiff must prove that (1) the defendant owed them a duty of care, (2) the defendant breached that duty, (3) the

---

<sup>14</sup> Defendants contend that certain negligence claims are barred by the economic loss rule. (Doc. No. 266 at 47-48, 47 n.24.) The Court will not address that issue because Defendants do not contend that the economic loss rule bars the Minnesota-law negligence claims. (*See* Doc. No. 267, App. A at 15 (negligence); *id.*, App. B at 12 (negligence per se).)

plaintiff was injured, and (4) the plaintiff's injury was proximately caused by defendant's breach. *Doe 169 v. Brandon*, 845 N.W.2d 174, 177 (Minn. 2014).

Individual Plaintiffs allege that “each Defendant owed Plaintiffs and the Class a duty to reasonably secure Plaintiffs’ and the Class’s Personal Information held by Change Healthcare and obtained by UHG and Optum upon its acquisition of Change Healthcare.” (Compl. ¶ 408.) Specifically, they allege that Defendants understood the need to adequately protect the Personal Information held on the Platform, and knew or should have known of the risks of deficient cybersecurity, creating a duty to exercise reasonable care to safeguard the Personal Information. (*Id.* ¶¶ 399-402, 410.) Defendants then breached that duty by failing to implement MFA, failing to internally monitor the network, and failing to segregate sensitive information. (*Id.* ¶ 409.) And as a “direct and proximate result of Defendants’ misconduct,” Individual Plaintiffs suffered harm. (*Id.* ¶¶ 412-13.)

Defendants contend that they did not owe Individual Plaintiffs any duty. (Doc. No. 266 at 40.) The existence of a duty of care is a question of law. *Doe 169*, 845 N.W.2d at 177. There is no general duty to safeguard data, but a duty to exercise reasonable care to protect that data arises if a defendant’s own conduct creates a foreseeable risk of data exposure. *E.g., Netgain*, 2022 WL 1810606, at \*10-11. Individual Plaintiffs plausibly allege that it was Defendants’ own conduct—the deficient cybersecurity—that created the risk. *See id.* at \*11 (finding that plaintiffs plausibly pled duty by alleging that defendant implemented deficient cybersecurity); *Chen v. Target Corp.*, No. 21-cv-1247, 2022 WL 1597417, at \*17 (D. Minn. May 19, 2022) (finding that

plaintiffs plausibly pled duty by alleging that defendant failed to implement proper security). Individual Plaintiffs explain how each Defendant owed a duty: Change Healthcare and Optum Insight by storing the data, and Optum and UHG by taking responsibility for the data. Individual Plaintiffs sufficiently pled duty based on foreseeable harm.

Defendants next contend that Individual Plaintiffs do not plausibly allege a breach of that duty, arguing that the mere existence of the Cyberattack does not prove negligence. (Doc. No. 266 at 45-47.) While a data breach is not always caused by negligence, Individual Plaintiffs have sufficiently pled that it was the cause here. *Compare In re MOVEit Customer Data Sec. Breach Litig.*, No. 23-md-3038, 2025 WL 2179475, at \*9 (D. Mass. July 31, 2025) (denying motion to dismiss similar allegations because specific cybersecurity failures plausibly pled breach of duty to take reasonable care), *with Crowe*, 2024 WL 6863341, at \*6, \*10 (dismissing claims because plaintiffs did not explain how the cybersecurity was deficient). The allegations explain in detail how Defendants breached. For example, if Defendants had limited access to the minimum access necessary, ALPHV would not have been able to create an administrative profile or install software. (Compl. ¶ 374.) Individual Plaintiffs sufficiently pled breach of the duty to exercise reasonable care.

For the reasons discussed above, causation and injury are also met. Individual Plaintiffs plausibly allege all elements of negligence, and the Court denies Defendants' motion to dismiss the negligence claim.<sup>15</sup>

### **C. Count II: Negligence Per Se**

Count II alleges that Defendants had a duty to provide adequate cybersecurity pursuant to the Federal Trade Commission Act ("FTC Act") and HIPAA, and that by breaching that duty, Defendants were negligent per se. (Compl. ¶¶ 417, 420.) The FTC Act prohibits unfair or deceptive trade practices. 15 U.S.C. § 45. HIPAA requires the protection of protected health information. 45 C.F.R. § 164.306 (2025).

Neither the FTC Act nor HIPAA provide for a private right of action. *FTC v. Johnson*, 800 F.3d 448, 452 (8th Cir. 2015); *Dodd v. Jones*, 623 F.3d 563, 569 (8th Cir. 2010). Minnesota law is unclear on whether the lack of a private right of action warrants dismissal of the claim. Some courts applying Minnesota law have dismissed for this reason. *See, e.g., Quaipe v. Brady, Martz & Assocs., P.C.*, No. 23-cv-176, 2024 WL 2319619, at \*3 (D.N.D. May 22, 2024); *Netgain*, 2022 WL 1810606, at \*15-16. Other courts have allowed claims to proceed under the general negligence per se framework. *E.g., Minnesota v. Fleet Farm LLC*, No. 22-cv-2694, 2024 WL 22102, at \*6 (D. Minn. Jan. 2, 2024); *Wiley ex rel. Wiley v. Fleet Farm LLC*, No. 24-cv-4135, 2025 WL 2601952, at \*25 (D. Minn. Sep. 9, 2025); *Perry v. Bay & Bay Transp. Servs., Inc.*,

---

<sup>15</sup> Count I also alleges breaches of duties to protect the Personal Information and to timely and accurately disclose of the Data Breach. (Compl. ¶¶ 403-04.) Having found that one theory of negligence survives, the Court need not consider alternative theories of duty. *See Fed. R. Civ. P. 8(d)(2)*.

650 F. Supp. 3d 743, 754-55 (D. Minn. 2023). In light of this unclear law, the Court declines to dismiss the negligence per se claims for lack of a private right of action. The Court now turns to the claims under the general negligence per se framework.

“In Minnesota, a violation of a statute or regulation gives rise to negligence per se if (1) the person harmed by that violation is among those the legislature sought to protect and (2) the harm suffered is of the type the statute or regulation was intended to prevent.” *Bay & Bay*, 650 F. Supp. 3d at 754. Both the FTC Act and HIPAA seek to protect the general public and are designed, at least in part, to protect against data breaches. *See id.* at 754 (noting that cybersecurity practices can be unfair under the FTC Act); *cf. In re SuperValu, Inc.*, 925 F.3d 955, 963 (8th Cir. 2019) [hereinafter *SuperValu II*] (noting that the FTC has brought actions against companies which fail to protect consumer data); *Negron v. Ascension Health*, No. 24-cv-669, 2025 WL 2710014, at \*10 (E.D. Mo. Sep. 23, 2025) (dismissing claim under FTC Act because FTC does not “legislate a standard of care for data security,” but keeping the HIPAA claim). Individual Plaintiffs are among the class of people the statutes sought to protect and suffered harm the statute was intended to prevent. The motion to dismiss as to the negligence per se count is denied.

**D. Count III: Third Party Beneficiary Breach of Contract**

Count III alleges that Defendants were subject to HIPAA security requirements via Business Association Agreements (“BAAs”) and failed to comply. (*Id.* ¶¶ 429-33.) Individual Plaintiffs bring a breach of contract claim as a third-party beneficiary, alleging

that the requirements in the BAA are intended to protect patients against the disclosure of their medical information and any resulting harm. (*Id.* ¶ 432.)

Generally, one who is not a party to a contract does not have rights under a contract, but an intended third-party beneficiary may acquire contractual rights. *Gelschus v. Hogen*, 47 F.4th 679, 686-87 (8th Cir. 2022). Therefore, to survive the motion to dismiss, Individual Plaintiffs must plausibly allege the existence of a contract, that the contract was intended for their benefit, and breach. *See Howry v. New Leaders, Inc.*, No. 18-cv-2648, 2019 WL 3804258, at \*2 (W.D. Tenn. Aug. 12, 2019); *cf. Lyon Fin. Servs., Inc. v. Ill. Paper & Copier Co.*, 848 N.W.2d 539, 543 (Minn. 2014) (requiring formation, performance of conditions precedent, and breach to be shown to sustain a breach of contract claim under Minnesota law).

### **1. Existence of a Contract**

To bring a third-party beneficiary claim to enforce a contract, there must be a contract to enforce. Individual Plaintiffs allege that “each Defendant must have entered into” at least one BAA. (Compl. ¶ 431.) They reason that because Defendants have access to patients’ PHI, Defendants must be in a BAA relationship with covered entities from whom Defendants obtain this information. (*Id.*) The complaint does not identify any specific party with whom Defendants may have contracted, nor any specific contract language which was breached. However, Individual Plaintiffs do identify HIPAA requirements, which must be included in any BAA, that were allegedly breached. (*Id.* ¶ 430.)

While these allegations are bare bones, the complaint does plausibly allege that each Defendant was a party to a BAA and that each BAA included the relevant security terms. *Cf. Horras v. Am. Cap. Strategies, Ltd.*, 729 F.3d 798, 804 (8th Cir. 2013) (dismissing breach of contract claim when plaintiff failed to plead any facts suggesting that a contract existed). For now, that is sufficient. *See Stasi v. Inmediata Health Grp. Corp.*, 501 F. Supp. 3d 898, 920 (S.D. Cal. 2020) (denying motion to dismiss “tenuous” breach of contract BAA claim because the substance of relevant terms was pled).

## **2. Intended Beneficiary**

“[A] third party is an intended beneficiary under a contract when it is appropriate to recognize third-party beneficiary rights to effectuate the intent of the parties to the contract, and either the duty owed or the intent-to-benefit test is satisfied.” *Caldas v. Affordable Granite & Stone, Inc.*, 820 N.W.2d 826, 833 (Minn. 2012), *superseded by statute on other grounds*, Act of Apr. 29, 2013, ch. 27, § 1, 2013 Minn. Laws 122, 122, *as recognized in*, *Hall v. City of Plainview*, 954 N.W.2d 254 (Minn. 2021). “A third party to the contract who does not meet this standard is merely an incidental beneficiary and has no right to enforce the contract.” *Id.* Under the intent-to-benefit test, the court must determine (1) whether the promisee intended to give the beneficiary the benefit of the promisor’s performance and (2) whether recognizing a right to performance by the beneficiary is appropriate to effectuate the intent of the contract. *Id.* Parties’ intent is determined from the language of the contract. *Id.* Because there is no specific contract between a Defendant and a covered entity from which to garner intent, the Court looks to the regulations controlling BAAs.

A covered entity may only share PHI with a business associate if the entities enter into a BAA in which the business associate promises to “appropriately safeguard the information.” 45 C.F.R. § 164.308(b)(1) (2025). The BAA must document these assurances and that the business associate agrees to comply with HIPAA security regulations. *Id.* §§ 164.308(b)(3), .314(a)(2). This indicates that protection of patient information is, at least in part, the reason that BAAs are formed. *See Barletti v. Connexin Software, Inc.*, No. 22-cv-4676, 2023 WL 6065884, ¶ 10 (E.D. Pa. Aug. 17, 2023) (denying motion to dismiss third-party beneficiary claim because contract expressed intent to store and secure plaintiffs’ medical data). *But see Kuchenmeister v. HealthPort Techs., LLC*, 309 F. Supp. 3d 1342, 1347 (noting, as dicta, that patients would be merely incidental beneficiaries while dismissing the claims because of a third-party disclaimer). The Court finds that BAAs are intended to benefit patients, including Individual Plaintiffs.

### **3. Breach**

As discussed above, Individual Plaintiffs allege that Defendants failed to comply with HIPAA by having deficient cybersecurity. Because they allege that the BAAs incorporated the same requirements as HIPAA security rules, such allegations suffice to show breach of the BAAs. (*See* Compl. ¶ 433.) However, because that breach is based entirely on statutory violations, Individual Plaintiffs’ breach of contract claim must fail.

When a federal statute lacks a private right of action, a breach of contract claim cannot be premised on a violation of that statute unless the breach also violated state laws. *See Astra USA, Inc. v. Santa Clara County*, 563 U.S. 110, 118-19 (2011). Put

differently, if a breach of contract claim goes beyond the federal violation, plaintiffs may continue that claim. *E.g., In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 1010 (N.D. Cal. 2016); *see also Dinerstein v. Google, LLC*, 484 F. Supp. 3d 561, 582-84 (N.D. Ill. 2020) (reviewing HIPAA preemption caselaw and concluding that state-law contract claims are not preempted). As mentioned above, HIPAA does not have a private right of action. *Dodd*, 623 F.3d at 569. Because the complaint only alleges violations of HIPAA as the basis for the breach of contract, the claim fails. *See Harris v. Mercy Health Network, Inc.*, No. 23-cv-195, 2024 WL 5055556, at \*10 (S.D. Iowa June 26, 2024) (collecting cases in which contractual claims based on HIPAA were dismissed).

Individual Plaintiffs attempt to save their claim by arguing that the breach is also based on generally applicable industry standards. (Doc. No. 329 at 76.) But they do not plead that the BAAs incorporated an obligation to follow generally applicable industry standards. Nor could they plausibly plead that the BAAs must have incorporated such an obligation because HIPAA does not require a promise to comply with industry standards in BAAs. Therefore, the Court grants Defendants' motion to dismiss Count III. This failure to plead warrants dismissal with prejudice because an amendment could not save the complaint. *See Chung Vue Xiong v. PHH Mortg. Corp.*, No. 13-cv-3128, 2014 WL 2893204, at \*7 n.6 (D. Minn. June 26, 2014).

#### **E. Count IV: Unjust Enrichment**

Count IV alleges that each Defendant received a monetary benefit from Individual Plaintiffs via the collection, use, sale, and analysis of their Personal Information. (Compl. ¶¶ 438-40.) “Unjust enrichment is an equitable doctrine that allows a plaintiff to

recover a benefit conferred upon a defendant when retention of the benefit is not legally justifiable.” *Herlache v. Rucks*, 990 N.W.2d 443, 450 (Minn. 2023) (citation modified). To state a claim, “the plaintiff must show that the defendant’s enrichment is illegal, unlawful, or morally wrong.” *Warren v. ACOVA, Inc.*, 21 N.W.3d 218, 242 (Minn. Ct. App. 2025). Additionally, the defendant must have benefited, but the benefit need not be conferred upon them directly by the plaintiff. *Id.* at 242-43; *see also Luckey v. Alside, Inc.*, 245 F. Supp. 3d 1080, 1099 n.26 (D. Minn. 2017) (discussing case law on direct conferral and concluding that direct benefit is not required).

Courts are split on whether PII and PHI can confer benefit. *Compare In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 592 (N.D. Ill. 2022) (collecting cases in which courts rejected the monetary value of PII theory, and dismissing unjust enrichment claim), *with In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1145 (C.D. Cal. 2021) (collecting cases in which courts allowed unjust enrichment claims on the theory of failure to protect PII, and denying motion to dismiss). Eighth Circuit precedent on unjust enrichment in the data breach context focuses on whether plaintiff paid extra for data security. *See Carlsen v. GameStop, Inc.*, 833 F.3d 903, 912 (8th Cir. 2016); *SuperValu II*, 925 F.3d at 966. Because Individual Plaintiffs did not pay Defendants, such precedent is unhelpful. Additionally, a court in this District found that PII was not a benefit sufficient to sustain an unjust enrichment claim. *Hall v. Centerspace, LP*, No. 22-cv-2028, 2023 WL 3435100, at \*6 (D. Minn. May 12, 2023). This case is inapposite because the plaintiff was an employee receiving

wages from the defendant, so the plaintiff received a direct benefit in return—here, the benefit to Individual Plaintiffs of claims processing is more tenuous.

The Court is persuaded that Individual Plaintiffs’ have sufficiently pled that their Personal Information was a benefit to Defendants in this scenario. Individual Plaintiffs explain that their data is valuable because it can be used by healthcare organizations for predicting outcomes and estimating costs. (*See* Compl. ¶¶ 181, 184, 296-97.) They also explain that access to the data was a major factor in UHG’s acquisition of Change Healthcare and benefitted each Defendant. (*See id.* ¶¶ 192-200.) These are plausible allegations that may be proven true through discovery. *See Chen*, 2022 WL 1597417, at \*14 (noting that the extent to which a benefit was retained is a question of fact).

However, the circumstances do not indicate that Defendants retained this benefit illegally or immorally. Individual Plaintiffs allege that they “would not have agreed to allow their providers to send their medical information to Defendants” had they know that Defendants did not have “reasonable safeguards to protect it.” (Compl. ¶ 445.) This allegation is contradicted by the fact that Individual Plaintiffs continue to have their medical providers send information through Defendants’ networks. (*See id.* ¶ 454.) Further, Individual Plaintiffs had no control over where providers sent their data. *Cf. In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1178 (D. Minn. 2014) (allowing unjust enrichment claim to continue because it was plausible that Plaintiffs would not have shopped at Target). Because Individual Plaintiffs have not shown that any benefit was retained unjustly, the Court grants Defendants’ motion to dismiss Count IV. The unjust enrichment claim is dismissed without prejudice.

## **F. Count V: Declaratory Judgment**

Individual Plaintiffs ask the Court to enter judgment declaring that “Defendants continue to owe a legal duty to secure Plaintiffs’ and Class members’ Personal Information and to timely notify Plaintiffs and Class members of a data breach under the common law, Section 5 of the FTC Act, HIPAA, and various state statutes” and that “Defendants continue to breach this legal duty by failing to employ reasonable measures to secure Plaintiffs’ and Class members’ Personal Information.” (Compl. ¶ 455.) Individual Plaintiffs further request that the Court “issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect Plaintiffs’ and Class members’ Personal Information.” (*Id.* ¶ 456.)

The Court finds that these requests are entirely duplicative of the negligence claims. Count I addresses Defendants’ alleged duty to secure the Personal Information and to notify. (*Id.* ¶¶ 403-04.) Count II addresses those duties under the FTC Act and HIPAA. (*Id.* ¶¶ 417, 420.) In both Counts I and II, Individual Plaintiffs note the continued risk of a future breach and request injunctive relief. (*Id.* ¶¶ 414-15, 426-27.) Those claims survived this motion to dismiss, so the issue will be settled later in litigation. *See, e.g., Great Am. Ins. Co. v. Twin Cities Dance & Ent., LLC*, No. 23-cv-767, 2024 WL 6475956, at \*6 (D. Minn. Jan. 16, 2024) (discussing redundant declaratory judgment claims). The Court therefore grants Defendants’ motion as to Count V and dismisses the declaratory judgment claim with prejudice. *See, e.g., Sorensen v. BlueSky*

*TelePsych, LLC*, No. 22-cv-2971, 2023 WL 3571937, at \*3, \*6 (D. Minn. May 19, 2023) (dismissing duplicative declaratory judgment claim with prejudice).

**G. State Statutory Claims<sup>16</sup>**

**1. Count XXIV: Violation of the Minnesota Deceptive Trade Practices Act<sup>17</sup>**

Count XXIV alleges that Defendants’ deficient cybersecurity violated the Minnesota Uniform Deceptive Trade Practices Act (“MUDTPA”) by deploying knowingly unreasonable data security measures. (Compl. ¶¶ 751-59.) The MUDTPA prohibits unfair methods of competition and unfair or unconscionable practices. Minn. Stat. § 325D.44, subdiv. 1(13) (2024).

To state a claim under the MUDTPA, Individual Plaintiffs must plausibly allege that Defendants’ deficient cybersecurity is “unfair or unconscionable.” *See id.* The Courts finds that Individual Plaintiffs have met that bar. The complaint explains how each Defendant failed to implement reasonable cybersecurity or sufficiently monitor Change Healthcare’s cybersecurity, which resulted in the Data Breach. *Cf. Bay & Bay*,

---

<sup>16</sup> Counts XXIV and XXV are brought on behalf of all Individual Plaintiffs and the Nationwide Subclass. However, Plaintiffs have not put forth any argument that the statutes are intended to apply extraterritorially, so the claims of the non-Minnesota-based Individual Plaintiffs are dismissed without prejudice. *E.g., Rouse v. H.B. Fuller Co.*, 694 F. Supp. 3d 1149, 1156-57 (D. Minn. 2023) (dismissing out-of-state claims under various Minnesota statutes).

<sup>17</sup> Briefing on state law causes of action did not specifically address the MUDTPA but discussed state consumer protection laws more generally. (*See* Doc. No. 266 at 58-69; Doc. No. 329 at 88-103.) The Court finds the general briefing sufficient to decide the motion as to the Minnesota-based Individual Plaintiffs. The Court will wait to analyze similar consumer protection laws until the claims of those states’ respective Individual Plaintiffs are considered.

650 F. Supp. 3d at 755 (finding that a failure to protect PII may be “unfair” under the FTC Act). Further, the complaint alleges that these deficiencies violated Defendants’ own policies. *Cf. Mohsen v. Veridian Credit Union*, 733 F. Supp. 3d 754, 773-74 (N.D. Iowa 2024) (denying motion to dismiss similar Iowa statutory claim in part because defendant had privacy policy). It is plausible that failing to implement reasonable security in violation of an entity’s policies is an unfair business practice.

The MUDTPA allows a person damaged by a deceptive trade act to pursue only injunctive relief and attorneys’ fees.<sup>18</sup> Minn. Stat. § 325D.45 (2024). To state a claim for injunctive relief, “a plaintiff must demonstrate that he himself faces risk of future harm.” *McDougall v. CRC Indus., Inc.*, 523 F. Supp. 3d 1061, 1076 (D. Minn. 2021). As discussed above, Individual Plaintiffs have alleged a threat of ongoing harm. *See Mekhail v. N. Mem’l Health Care*, 726 F. Supp. 3d 916, 932 (D. Minn. 2024) (noting that a showing of future harm for MUDTPA purposes is “seemingly indistinguishable” from a showing for Article III purposes (citation modified)). Defendant’s motion to dismiss the MUDTPA claim is denied.

## **2. Count XXV: Violation of the Minnesota Health Records Act**

Finally, Count XXV alleges that Defendants are liable under the Minnesota Health Records Act (“MHRA”) because they caused the unauthorized release of Individual Plaintiffs’ medical records. (Compl. ¶ 771.) The MHRA prohibits healthcare providers,

---

<sup>18</sup> Individual Plaintiffs seek monetary and non-monetary damages. (*Id.* ¶ 763.) Individual Plaintiffs concede that the monetary request is improper. (*See* Doc. No. 329 at 93.) The Court therefore dismisses the request for monetary relief with prejudice.

and those who receive health records from a provider, from releasing a patient's health records without consent or specific authorization in law. Minn. Stat. § 144.293, subdiv. 2 (2024). Release can be either negligent or intentional. *Id.* § 144.298, subdiv. 2(1).

“Health record” is defined broadly to include “any information” that relates to a patient's health condition, provision of health care, or payment for health care. *Id.* § 144.291, subdiv. 2(c); *see also Holtzbauer v. Allina Health Sys.*, 23 N.W.3d 608, 613-20 (Minn. Ct. App. 2025) (discussing the breadth of the term's definition). The Personal Information stolen in the Data Breach includes medical and payment information. This is sufficient to allege that Defendants possessed their health records. *See In re Grp. Health Plan Litig.*, 709 F. Supp. 3d 707, 713 (D. Minn. 2023) (denying motion to dismiss because of the broad definition of “health record”).

Individual Plaintiffs have also sufficiently alleged that the Personal Information was released. Through the Data Breach, cybercriminals got access to Individual Plaintiffs' data, which was then posted on the dark web. By failing to protect the data, Defendants allowed for the Personal Information to be taken from the network and available to outside actors. *See generally Larson v. Nw. Mut. Life Ins. Co.*, 855 N.W.2d 293, 302 (Minn. 2014) (defining “release” as letting go or making available for use). Defendants argue that because the Personal Information was stolen by cybercriminals, it was not affirmatively released. (Doc. No. 266 at 68.) Defendants rely on *Netgain*, in which the court found that theft by cybercriminals was not an affirmative release as required by the statute. 2022 WL 1810606, at \*16. The Court respectfully disagrees with the explanation in *Netgain*. The statute explicitly provides for liability when release is

either negligent or intentional. *See* Minn. Stat. § 144.298, subdiv. 2(1) (2024). The act of negligently utilizing deficient cybersecurity which results in a data breach imposes liability, in this Court’s opinion.<sup>19</sup>

The Minnesota-based Individual Plaintiffs have sufficiently alleged a violation of the MHRA. Defendants’ motion to dismiss Count XXV as to the Minnesota-based Individual Plaintiffs is denied.

### CONCLUSION

At the motion to dismiss stage, the Court accepts the facts alleged in the complaint as true and views those allegations in the light most favorable to the plaintiff. Under that standard, Individual Plaintiffs have sufficiently alleged negligence, negligence per se, violation of the MUDPTA, and violation of the MHRA. However, Individual Plaintiffs’ claims of third-party beneficiary breach of contract, unjust enrichment, and declaratory judgment fall short. Those claims are dismissed.

### ORDER

Based upon the foregoing and the record in this case, **IT IS HEREBY**

**ORDERED** that:

1. Defendants’ motion to dismiss Individual Plaintiffs’ claims (Doc. No. [256]) is **GRANTED IN PART AND DENIED IN PART** as follows:

---

<sup>19</sup> Further, the MHRA “must be construed to protect the privacy of a patient’s health records” in a manner “more stringent” than HIPAA. Minn. Stat. § 144.2925 (2024). Having found that Individual Plaintiffs sufficiently pled a claim of negligence per se for violation of HIPAA in Count II, the Court finds that claims under the MHRA must also survive.

a. The motion is granted as to Counts III, IV, and V as to Plaintiffs Brooks, Powers, and Allen **ONLY**.

b. The motion is granted as to Counts XXIV and XXV as to the non-Minnesota-based Individual Plaintiffs **ONLY**.

c. The motion is respectfully denied as to Counts I, II, XXIV, and XXV as to Plaintiffs Brooks, Powers, and Allen **ONLY**.

2. Plaintiffs Brooks, Powers, and Allen's claims in Counts III and V are **DISMISSED WITH PREJUDICE**.

3. Plaintiffs Brooks, Powers, and Allen's claims in Count IV are **DISMISSED WITHOUT PREJUDICE**.

4. The non-Minnesota-based Individual Plaintiffs' claims in Counts XXIV and XXV are **DISMISSED WITHOUT PREJUDICE**.

5. The parties shall submit response and reply briefing on the non-Minnesota-based Individual Plaintiffs' claims under their respective home state's laws.

a. The parties are directed to meet and confer on an appropriate timeline for this briefing and to file a stipulation on the matter by January 16, 2026.

b. The Court reserves ruling on the motion to dismiss as to the non-Minnesota-based Individual Plaintiffs until such briefing is received.

Dated: December 19, 2025

s/Donovan W. Frank  
DONOVAN W. FRANK  
United States District Judge