John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 92101
Telephone: (858) 209-6941
jnelson@milberg.com

Additional Signature blocks listed below.

Attorneys for Plaintiff and Putative Class

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

A.H., individually and on behalf of all others similarly situated, Plaintiff, v. MEDTRONIC MINIMED, INC. and MINIMED DISTRIBUTION CORP., Defendants.	Case No. **CLASS ACTION COMPLAINT FOR DAMAGES, INJUNCTIVE RELIEF, & EQUITABLE RELIEF FOR:** **(1) Common Law Invasion of Privacy – Intrusion Upon Seclusion** **(2) Breach of Confidence** **(3) Breach of Fiduciary Duty** **(4) Negligence** **(5) Breach of Implied Contract** **(6) Breach of Implied Covenant & Fair Dealing** **(7) Unjust Enrichment** **(8) Violation of Electronic Communications Privacy Act ("ECPA") –Unauthorized Interception, Use, & Disclosure;** **(9) Violation of ECPA – Unauthorized Divulgence;** **(10) Violation of Title II of the ECPA 18 U.S.C. § 2702, *et seq*. -Stored Communications Act** **(11) Violations of Cal. Penal Code §630, *et seq.* California Invasion of Privacy Act ("CIPA")**

(12) Violation of NY Gen. Bus. Law §349 *et seq*.

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff A.H. brings this class action lawsuit, on behalf of himself and similarly situated individuals who used the InPen system, against Defendants Medtronic MiniMed, Inc., and MiniMed Distribution Corp. (collectively, "Defendants" or "MiniMed"). The allegations set forth in this class action complaint are based on Plaintiff's personal knowledge, investigation of undersigned counsel, and upon information and belief.

NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit to address MiniMed's transmission and disclosure of Plaintiff's and Class Members' personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "Private Information") to Google LLC d/b/a Google ("Google") and other third parties via tracking and authentication technologies—including Google Analytics, Crashlytics, Firebase Authentication, and related tools ("Tracking Tools")—installed on its Website and/or mobile applications, including the InPen Diabetes Management iOS and Android mobile applications (the "App," and collectively, the "Digital Platforms").

2. Information about a person's health is among the most confidential and sensitive information in society, and its mishandling can have serious consequences, including embarrassment, discrimination, and denial of insurance coverage.

3. MiniMed promotes its Digital Platforms and corresponding medical devices as providing an integrated system that combines insulin pumps and continuous glucose monitoring for people living with type 1 and type 2 diabetes.

4. MiniMed encourage patients to sign up for their App, promoting it and

related online services as aiding patients with their medical care and use of the InPen[1] system—a smart insulin delivery system or "pen" that combines a reusable, Bluetooth-enabled insulin pen with an intuitive mobile app to help people with type 1 or type 2 diabetes take the right amount of insulin, at the right time.

The InPen System Description

5. The InPen system is comprised of the InPen device and corresponding InPen App, which is a diabetes management tool that helps patients track their insulin doses throughout the day and calculate how much insulin they need based on their reported glucose reading and carbohydrate intake. In addition to helping patients track and record their daily readings, it also provides a platform for patients to share and communicate their information with their healthcare team.[2]

6. The App also automatically records the size and timing of insulin doses, provides reminders and alerts when insulin is not taken, includes personalized settings for insulin dose calculation, and can be integrated with other diabetes technologies, including a continuous glucose monitor (CGM) or through blood glucose meters (BGM).[3]

7. For the App to work effectively with the patient's healthcare provider, the patient must set up their therapy settings, which are provided by their healthcare provider and input by the patient.[4] As such, patients use the App as a means of communicated important health information with their healthcare provider.

8. Based on its solicitations and representations, Plaintiff and Class Members

---

[1] InPen is a registered trademark owned by Companion Medical, Inc. References to InPen contained herein will not include the trademark symbol ™.

[2] Companion Medical. 2023.*InPen System Instructions for Use.* Companion Medical. https://www.medtronicdiabetes.com/sites/default/files/library/download-library/user-guides/InPen-user-guide.pdf

[3] *Id.*

[4] *Id.*

used the InPen System to treat diabetes and communicate with their care providers as part of their ongoing medical care and treatment ("InPen Users" or "Patients").

9. MiniMed collects and stores InPen Users' Private Information and medical records, and in doing so, has a duty to ensure the information is kept confidential.

10. To assuage any concerns Patients may have regarding their Private Information, MiniMed makes several promises, stating it "is committed to maintaining the privacy of your Protected Health Information" and "will only use or disclose (share) your Protected Health Information as described" in its Notice of Privacy Practices.[5]

11. MiniMed represents it will only use or disclose Protected Health Information without a Patients' written authorization in limited circumstances—none of which apply here—and does not include or mention Tracking Technologies in the enumerated list or otherwise represent that information will be shared with Google.[6]

12. MiniMed is duty bound to maintain the confidentiality of such information, as codified by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[7]

13. Yet, despite its unquestionable obligation to protect the confidentiality and security of Patients' Private Information, MiniMed made the conscious decision to use Tracking Tools on its Digital Platforms to acquire very sensitive, personal information and data about Plaintiff's and Class Members' medical conditions and communications, which was disseminated to third parties, including Google, for marketing and analytics

---

[5] *Notice of Privacy Practices,* https://www.medtronicdiabetes.com/notices (last accessed Aug. 18, 2023).

[6] *Id.*

[7] HIPAA, Pub. L. No. 104-191, 110 Stat. 1936 (1996), and regulations of the United States Department of Health and Services ("HHS") promulgated thereunder, are designed to protect the confidentiality and guard against the unauthorized disclosure of medical records, patient health care information and other individually identifiable healthcare information.

purposes and, ultimately, to increase revenue and profits. [8]

14. For nearly a decade, data brokers have specifically sought to identify diabetes patients, and a report published by the Federal Trade Commission ("FTC") in 2014 named diabetes among one of 37 commonly used data categories.[9]

15. Although the full scope of MiniMed's data monetization and sharing practices is presently unknown, the information it illegally sent to third parties can be associated with other data to create highly detailed user profiles for marketing and other commercial purposes—none of which benefit InPen Users.

16. MiniMed's disclosures of PII and PHI to Google is particularly problematic because Google provides webservices—such as YouTube and Gmail—that give it access to InPen users' real identity and device identifiers. Plaintiff used his mobile device to access the App, and he also uses it to access his Gmail account. As a result, his PII and PHI was automatically linked to his real identity. Even if Plaintiff did not possess a Gmail account, Google would have nonetheless received information that allows it to

---

[8] MEDTRONIC *Case Study: 3 ways data and insights can improve care and costs across health systems* (January 2022), available at https://www.medtronic.com/content/dam/medtronic-wide/public/brand-corporate-assets/resources/3-ways-data-driven-insights-case-study_corpmark_mdt.pdf (last visited Aug. 18, 2023)(stating, We are committed to applying data analytics, machine learning, and artificial intelligence to improve healthcare technology globally. And by partnering with health systems in new ways — from acting on population health data to ***gathering insights through connected technologies*** — we believe we can help improve experiences for patients and clinicians. With advanced data and analytics, our health system partners get the best of both worlds: greater personalization of care and insights that can be applied broadly for extraordinary outcomes. ***The payoff is clear and has sparked our investment in technology to gather and process data."*** (emphasis added).

[9] FEDERAL TRADE COMMISSION, *Data Brokers: A Call for Transparency and Accountability* (May 2014), available at https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (last accessed Aug. 25, 2023).

individually identify him.

17. MiniMed chose to unlawfully intercept and transmit Patients' Private Information in this manner because it knew patients would *not* provide their Private Information or use the InPen App to communicate with their care providers if they were informed of what MiniMed intended to do with it.

18. Healthcare companies have been warned as far back as at least February 2020[10] that they may be disclosing Private Information to digital marketing companies by embedding and using Tracking Tools. Despite those warnings and its own use of such Tracking Tools, MiniMed did not publicly acknowledge its collection and dissemination of its Users' Private Information until April of 2023.[11]

19. MiniMed also posted a Notice (the "Notice"), stating that the "priority is to ensure users can continue to access diabetes management tools on their InPen App accounts in a secure manner," and thus it was:

> writing to share some important information regarding a recent data privacy incident involving the InPen™ Diabetes Management iOS and Android mobile applications.
> . . .
>
> **What happened?**
>
> On February 13, 2023, Medtronic Diabetes determined that tracking and authentication technologies used on the InPen™ App, including Google Analytics for Firebase ("Google Analytics"), Crashlytics for Firebase

---

[10] Molly Osberg & Dhruv Mehrotral, *The Spooky, Loosely Regulated World of Online Therapy*, JEZEBEL (Feb. 19, 2020), available at https://jezebel.com/the-spooky-loosely-regulated-world-of-online-therapy-1841791137 (last visited March 21, 2023); *see also* Timothy M. Hale, PhD & Joseph C. Kvedar, MD, *Privacy and Security Concerns in Telehealth*, (Dec. 2014), https://journalofethics.ama-assn.org/article/privacy-and-security-concerns-telehealth/2014-12, AMA JOURNAL OF ETHICS (last visited Mar. 21, 2023) (illustrating that problems with privacy and telehealth apps started to surface as early as 2014).

("Crashlytics") and Firebase Authentication (collectively referred to in this letter as "Google Services") disclose certain details about a user's actions within the InPen™ App; particularly for users that are logged into their Google accounts at the same time as the InPen™ App and have shared their identity or other online activity with Google. Upon learning about this incident, we promptly launched an internal investigation to better understand what user information had been shared with Google through use of the Google Services.

In an effort to deliver high quality services to patients, Medtronic Diabetes used the services of Google Analytics and Crashlytics to understand how users interact with the InPen™ App. These technologies were designed to gather information so that we can better identify technical issues, assess the performance of the application and understand user needs and preferences to provide needed care to our customers. This information is reviewed by us at a consolidated level, not at the individual level, and does not directly identify individual patient information. Medtronic Diabetes also used the services of Firebase Authentication to securely authenticate users logging into the InPen™ App.

We recently learned that Google Analytics and Crashlytics transmitted certain user information to Google once a user logged into their account, and Firebase Authentication transmitted certain user information to Google in connection with a user's registration on the InPen™ App.

How do I know If I was affected?

Out of an abundance of caution, Medtronic Diabetes is contacting all users who have registered for, or used, an InPen™ account since September 2020, as they may have been affected. You may have been impacted differently based on your choice of browser; the configuration of your browsers; your blocking, clearing or use of cookies; whether you have Google accounts; whether you were logged into Google; and the specific actions you took on the platform.

What information was involved?

The following information may have been involved: your email address, IP address, phone number, InPen™ App user name and password, timestamp information related to specific InPen™ App events, and certain unique identifiers tied to your InPen™ account or mobile device (specifically, your

> unique Medtronic Diabetes user identifier (a unique string of numbers or characters assigned to each user of the InPen™ App by Medtronic Diabetes)), unique numbers attributed to each instance the InPen™ App is downloaded to a particular device, and identifiers tied to your mobile device (such as mobile advertising IDs (MAIDs), Identifiers for Advertisers (IDFAs), Android Advertising IDs for Android devices (AAIDs), and Identifier for Vendors for iOS devices (IDFVs)).[12]

20. MiniMed's conduct violates its own Privacy Policy, which promises Patients' Private Information will not be shared for marketing purposes unless it first receives written authorization for that disclosure.[13]

21. Despite this representation (as well as many other similar ones in the Privacy Policy and elsewhere), MiniMed has publicly acknowledged its use of invisible Tracking Tools on its Digital Platforms since September 2020.

22. In short, MiniMed intentionally chose to put its profits over its Patients' privacy so it could access and monetize their valuable data for future marketing efforts.

23. The disclosure of Plaintiff's and Class Members' Private Information via the Tracking Tools undermines the letter and purpose of HIPAA's "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule"), which governs how healthcare providers must safeguard and protect Private Information. [14]

24. The HIPAA Privacy Rule sets forth policies to protect all Individually Identifiable Health Information ("IIHI") that is held or transmitted by a covered entity such as MiniMed, and 18 HIPAA Identifiers are considered personally identifiable information because they can be used to identify, contact, or locate a specific person or

---

[12]https://app.medtronicdib.mdtpatient.com/e/es?s=357929245&e=898604&elqTrackId=b0ce7494b5bd47ad9b9c672c71086a1c&elq=1943108c08db4c6f99194c7778a8b25e&elqaid=8161&elqat=1.

[13] *Notice of Privacy Practices,* https://www.medtronicdiabetes.com/notices.

[14]HHS.gov, The HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (last visited August 10, 2023).

can be used with other sources (such as a person's Google account) to identify a single individual. When IIHI is used in conjunction with one's health or condition, health care, and/or one's payment for that health care, it becomes PHI.[15]

25. While healthcare entities regulated under HIPAA may use third-party tracking tools, they can do so only in a very limited way. Simply put, covered entities such as the MiniMed, are ***not*** permitted to use Tracking Tools in a way that exposes patients' Private Information to any third party without express and informed consent.

26. In fact, the Office for Civil Rights (OCR) at HHS has made clear, in a recent bulletin entitled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, that the unlawful transmission of such protected information violates HIPAA's Privacy Rule:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[16]

---

[15] *Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html, HHS.GOV (last visited Mar. 21, 2023) (HIPAA Identifiers include name; address (all geographic subdivisions smaller than state, including street address, city county, and zip code); all elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age); telephone numbers; email address; medical record number; health plan beneficiary number; account number; device identifiers and serial numbers; web URL; internet protocol (IP) address; and any other characteristic that could uniquely identify the individual).

[16] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business*

27. Moreover, MiniMed breached its statutory and common law obligations to Plaintiff and Class Members by, *inter alia*,: (i) failing to adequately review its marketing programs and web-based technology to ensure its Digital Platforms were safe and secure; (ii) failing to remove or disengage technology that was known and designed to share Patients' information; (iii) failing to obtain the written consent of Plaintiff and Class Members to disclose their Private Information to Google and/or other third-parties; (iv) failing to take steps to block the transmission of Plaintiff's and Class Members' Private Information via Tracking Tools; (v) failing to warn Plaintiff and Class Members that their Private Information was being shared with third parties without express consent; and (vi) otherwise failing to design and monitor its Digital Platforms to maintain the confidentiality and integrity of patient Private Information.

28. As a result of MiniMed's conduct, Plaintiff and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) diminution of value of the Private Information; (iv) statutory damages; and (v) the continued and ongoing risk to their Private Information.

JURISDICTION & VENUE

29. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs, and minimal diversity exists because at least one class member and one of the Defendants are citizens of a differing states.

30. This Court also has federal question jurisdiction pursuant to 28 U.S.C. § 1331 since this suit is brought under the laws of the United States, i.e., the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq*. and the Federal Wiretap Act, 18 U.S.C.

Associates, available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html, HHS.GOV (emphasis added) (last visited June 4, 2023).

§§ 2511, *et seq*., and supplemental jurisdiction pursuant to 28 U.S.C. § 1367 over the remaining state common law and statutory claims as these state law claims are part of the same case or controversy as the federal statutory claim over which the Court has original jurisdiction.

31. The State of California has personal jurisdiction over MiniMed because Medtronic MiniMed Inc.'s principal place of business and headquarters is in this District, it employs California residents, and it conducts business throughout the state of California. Additionally, the InPen system was developed and manufactured by Companion Medical Inc., which was headquartered and maintained its principal place of business in San Diego prior to its acquisition by Medtronic MiniMed Inc.

32. Venue is proper in this District pursuant to 28 U.S.C.§ 1391(b)(1) because MiniMed's principal place of business is in this judicial district, and many of the acts and/or omissions giving rise to the claims asserted herein occurred in this judicial district. More specifically, MiniMed's decisions regarding the InPen device and App were made in this District, InPen Patients are directed to contact MiniMed by mail in this District, and decisions concerning its other diabetes-related wearable devices were made in this District.

PARTIES

Plaintiff A.H.

33. Plaintiff A.H. is an individual residing in the State of New York who at all relevant times was a citizen and resident of New York.

Defendant Medtronic MiniMed, Inc.

34. Defendant Medtronic MiniMed, Inc. is a healthcare company incorporated in Delaware with its principal place of business and headquarters located at 18000 Devonshire Street, Northridge, California 91325.

Defendant MiniMed Distribution Corp.

35. Defendant MiniMed Distribution Corp. is a healthcare company incorporated in Delaware with its principal place of business and headquarters located at

18000 Devonshire Street, Northridge, California 91325.

COMMON FACTUAL ALLEGATIONS

MiniMed Improperly Discloses Patients' PHI & Assists with Intercepting Communications.

36. MiniMed's InPen system and Digital Platforms collect a treasure trove of personal data patients communicate in relation to their healthcare, which MiniMed secretly mines, transmits, and intercepts for its own benefit.

37. MiniMed promotes its App with the goal of increasing its profitability and purposely installed Tracking Tools on its Digital Platforms, using and/or programming them in a manner that caused Patients' Private Information and protected communications to be transmitted to third parties, including Google, without Plaintiff's and Class Members' knowledge or consent.

38. Plaintiff and Class Members did not intend or have any reason to suspect their Private Information would be shared with Google and other third parties, or that MiniMed was tracking their every communication and disclosing the same to third parties when they communicated highly sensitive information via MiniMed's Digital Platforms. By law, Plaintiff and Class Members are entitled to privacy in their Private Information and confidential communications.

39. Due to Plaintiff and Class Members' sensitive relationship with MiniMed, Plaintiff and Class Members have a heightened expectation that their Private Information will be kept confidential and not shared with unauthorized third parties.

40. Despite this—as now admitted in the Notice—MiniMed knowingly disclosed Plaintiff's and Class Members' Private Information to Google and other third parties, and it continued engaging in this course of conduct despite knowledge that doing so would run afoul of HIPAA, related privacy laws, and its own Privacy Policies.

41. Upon information and belief, MiniMed intercepted, transmitted, disclosed, and assisted the interception of Plaintiff's and Class Members': (1) status as a MiniMed user (and thus as a person with diabetes); (2) information about their specific medical

conditions and treatments and related health information (such as their insulin use); (3) name, phone number, email address, date of birth, IP address, and other sensitive personal and demographic information; and (4) unique identifiers tied to their InPen account or mobile device.

42. Thus, MiniMed deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented Tracking Tools to surreptitiously track, record, and disclose their Private Information; (2) disclosed their Private Information to Google, and/or other unauthorized third parties and assisted third parties in intercepting patients' Private Information; and (3) undertook this pattern of conduct without notifying them and without obtaining their express written consent.

Medtronic's Conduct, Including its Implementation and Use of the Tracking Tools on its Digital Platforms, Violates its Own Privacy Policies because Private Patient Information was Automatically Transmitted to Google for Marketing Purposes.

43. In MiniMed's Privacy Policies, MiniMed promises Private Information will be kept secure and confidential, and that it will only disclose Private Information under certain circumstances.[17] The Privacy Policies also promise that Plaintiff's and Class Members' Private information will not be shared for marketing purposes without prior, written permission. ***None of this is true***.

44. Specifically, MiniMed publishes a Notice of Privacy Practices informing patients that it will only use and disclose PHI in the following ways:

> Treatment: Medtronic may share PHI with third parties for all treatment related purposes. For example, Medtronic may fax or securely email documents with your treating physicians or other health care providers involved in your care about product orders or health care services.
>
> Payment: Medtronic may share your PHI to bill and obtain payment from health plans or other entities, including for example, federal health care

[17] Notice of Privacy Practices, *https://www.medtronicdiabetes.com/notices* (last accessed Aug. 18, 2023).

> programs (Medicare and Medicaid).
>
> Health Care Operations: Medtronic may utilize and share your PHI to run its business, improve your treatment and contact you when necessary. For example, Medtronic may use your PHI to conduct quality or compliance audits, to review the quality of Medtronic products and services.[18]

45. MiniMed's Privacy Policy does ***not*** permit it to use and disclose its patients' Private Information for marketing purposes, much less to one of the largest online advertisers in the world. Rather, it represents:

> Medtronic will obtain your authorization or consent before using your PHI or disclosing it to persons or organizations outside of Medtronic in the following situations:
>
> - For marketing or promotional purposes
> - Sale of your PHI
> - Any other reason not described in this Notice.[19]

46. Medtronic promises that it will not disclose PHI of its users' Private Information without their authorization and consent is false and misleading. Plaintiff and Class Members have not provided MiniMed with written permission to share their Private Information for marketing purposes. Despite that fact, MiniMed has admitted that it shared such information with Google and other third parties.

47. MiniMed's "U.S. Patient Privacy Principles" further provides:

> Medtronic is the world leader in medical technology providing lifelong solutions for people with chronic disease. To perform our jobs, we may create, develop or receive information about patients' experiences with our products and services in a variety of situations, including:
>
> - We provide therapy or technical support for our products.
> - We receive questions and suggestions about our products and services

[18] *Id*.

[19] *Id*. (emphasis added).

from patients and physicians.
- We enroll patients in our clinical trials.
- We collect information as required by the FDA and other governmental authorities to assure safe and effective use of our products.
- We collect, analyze, and re-analyze our data in a continuous effort to improve the design, quality and functioning of our devices.

Preservation of, and respect for, our customers' trust is critical to our continued success. We will always treat such patient information:

- Confidentially, according to applicable laws.
- Appropriately, according to the promises we make to our customers.
- Respectfully, in honor of our patients' willingness to trust us to use sensitive information to oversee the quality, safety and effectiveness of the devices that they make part of their daily lives.[20]

48. MiniMed also makes the following promises:

Information Security: We maintain appropriate physical, technical and administrative security standards and procedures to safeguard our patient data and systems. Our employees are educated on the importance of our privacy and security policies and must comply with them. Employees are permitted to access and use only the patient information they need to perform their job duties.

Data Integrity and Access: The lawful operation of our business demands that we take steps to assure the accuracy and integrity of the data that we use. Where our data are used in making decisions that may affect the subject of the information, as in device tracking, we assure that the subject has access to inspect and correct the data in accord with applicable laws.

Medtronic is committed to supporting our customers in their efforts to protect the confidentiality of protected health information. We expect our employees to comply with our customers' instructions regarding their policies that govern visitor behavior in their facilities – and we expect to be accountable to our customers for appropriately sanctioning our employees who fail to do so.[21]

---

[20] Medtronic, U.S. Patient Privacy Principles, https://www.medtronic.com/us-en/about/corporate-governance/us-patient-privacy-principles.html.
[21] *Id.*

49. MiniMed violated its own privacy policies by unlawfully intercepting and disclosing Plaintiff's and Class Members' Private Information to Google and other third parties without first obtaining Plaintiff's and Class Members' consent or authorization.

50. Even non-Google users can be individually identified via the information gathered on the Digital Platforms, particularly since Google received Patients' names, email addresses, IP addresses, personal device identifying information, and related identifiers—all of which allow their information to be individually attributed to them.

51. MiniMed also failed to adhere to its own policies by representing that it would notify affected victims in the event of a breach when, in reality, it undertook a course of conduct that resulted in significant delay.

52. Despite its explicit promises to the contrary, MiniMed allowed third parties to "listen in" on confidential communications, to intercept the contents of those communication, and further use the information for advertising purposes—the exact information it represented it would safeguard and keep confidential.

MiniMed's Use of the Tracking Tools Violates HIPAA

53. 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.[22]

54. In this case, the disclosure of a person's status as an InPen user is, in and of itself, a HIPAA violation because it reveals that the individual has been diagnosed with a specific medical condition (diabetes) and is receiving a specific type of medical treatment for that medical condition (insulin).[23]

---

[22] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

[23] The mere fact that an individual is receiving a medical service, *i.e.*, is a patient of a

55. The Privacy Rule broadly defines PHI as 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.

56. 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.

57. Under the HIPAA 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:

---

particular entity, can be PHI, and the Department of Health and Human Services has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source such as a phonebook, "[i]f such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI." *See Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, (Nov. 26, 2012) at 5 , available at https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html, HHS.GOV (last visited June 4, 2023).

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

P. Any other unique identifying number, characteristic, or code… and . . .” 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.

58. The HIPAA Privacy Rule requires MiniMed to maintain appropriate safeguards to protect the privacy of PHI, sets limits and conditions as to its usage and disclosure, and further defines when it is acceptable to use or disclose PHI without authorization. 45 C.F.R. §§ 160.103, 164.502.

59. In 2003, the HHS further instructed:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual’s written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party’s own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*. (Emphasis added). https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/covered entities/marketing.pdf (April 3, 2003) (last visited Aug. 3, 2022).

MiniMed violated this rule by disclosing Plaintiff and Class Members' information to Google—one of the largest online advertisers in the world—without first obtaining their written authorization.[24]

60. HIPAA also requires Defendants to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(c), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1). MiniMed further failed to comply with other HIPAA safeguard regulations by:

a. Failing to ensure the confidentiality and integrity of electronic PHI that MiniMed created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. section 164.308(a)(1);

c. Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to MiniMed in violation of 45 C.F.R. § 164.308(a)(6)(ii);

d. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. §

---

[24] For decades, HHS has repeatedly instructed that patient status is protected by the HIPAA Privacy Rule: "The sale of a patient list to a marketing firm" is not permitted under HIPAA. See 65 Fed. Reg. 82717 (Dec. 28, 2000); "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which includes disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002); and it would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 Fed. Reg. 5642 (Jan. 25, 2013).

164.306(a)(2);

e. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI not permitted under the privacy rules pertaining to individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

f. Failing to ensure compliance with HIPAA security standard rules requiring adequate workforce comprehensive training in violation of 45 C.F.R. §§ 164.306(a)(4), 164.530(b), and 164.308(a)(5); and

g. Failing to design, implement, and enforce policies and procedures that would establish physical and administrative safeguards to reasonably safeguard PHI in violation of 45 C.F.R. § 164.530(c).

61. In addition, the Office for Civil Rights (OCR) at HHS has issued a Bulletin to highlight the obligations of HIPAA covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies.[25]

62. The Bulletin expressly provides that "**[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.**"[26]

63. Tracking technology vendors like Google are considered business associates under HIPAA where, as here, they provide services to Defendants and receive and maintain PHI.

Furthermore, tracking technology vendors are business associates if they

[25] *See* HHS.gov, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates (Dec. 1, 2022), available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Aug. 5, 2022).

[26] *Id.* (emphasis in original).

> create, receive, maintain, or transmit PHI on behalf of a regulated entity for a covered function (*e.g.*, health care operations) or provide certain services to or for a covered entity (or another business associate) that involve the disclosure of PHI. In these circumstances, regulated entities must ensure that the disclosures made to such vendors are permitted by the Privacy Rule and enter into a business associate agreement (BAA) with these tracking technology vendors to ensure that PHI is protected in accordance with the HIPAA Rules. For example, if an individual makes an appointment through the website of a covered health clinic for health services and that website uses third party tracking technologies, then the website might automatically transmit information regarding the appointment and the individual's IP address to a tracking technology vendor. In this case, the tracking technology vendor is a business associate and a BAA is required.[27]

64. The Bulletin further explained that health care providers violate HIPAA when they use tracking technologies that disclose an individual's identifying information (like an IP address) even if no treatment information is included and even if the individual does not have a relationship with the health care provider:

> How do the HIPAA Rules apply to regulated entities' use of tracking technologies?
>
> Regulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a regulated entity's website or mobile app, including individually identifiable health information (IIHI) that the individual providers when they use regulated entities' websites or mobile apps. This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code. All such IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. **This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the**

[27] *Id.*

> **regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care**.[28]

65. HIPAA applies to MiniMed's webpages with tracking technologies even outside the App:

> Tracking on unauthenticated webpages
>
> [T]racking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include: The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal **… [and pages] that address[] specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances**. For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a health care provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.[29]

66. HHS also explained in the Bulletin that tracking technologies on health care providers' patient portals "generally have access to PHI" and may access diagnoses and treatment information, in addition to other sensitive data:

> Tracking on user-authenticated webpages
>
> Regulated entities may have user-authenticated webpages, which require a user to log in before they are able to access the webpage, such as a patient

---

[28] *Id.* (emphasis added).

[29] *Id.* (emphasis added).

> or health plan beneficiary portal or a telehealth platform. **Tracking technologies on a regulated entity's user-authenticated webpages generally have access to PHI.** Such PHI may include, for example, an individual's IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage. Tracking technologies within user-authenticated webpages may even have access to an individual's diagnosis and treatment information, prescription information, billing information, or other information within the portal. Therefore, a regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to only use and disclose PHI in compliance with the HIPAA Privacy Rule and must ensure that the electronic protected health information (ePHI) collected through its website is protected and secured in accordance with the HIPAA Security Rule.[30]

67. The Bulletin is not a pronouncement of new law, but instead reminded covered entities and business associates of their longstanding obligations under existing guidance. The Bulletin notes that "it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors," then explains how online tracking technologies violate the same HIPAA rules that have existed for decades.[31]

68. In other words, HHS has expressly stated that MiniMed violated HIPAA Rules by implementing the Tracking Tools.

MiniMed Violated Industry Standards.

69. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

---

[30] *Id.* (emphasis added).

[31] *Id.* (citing, e.g., Modifications of the HIPAA [Rules], Final Rule," 78 FR 5566, 5598, a rulemaking notice from January 25, 2013, which stated: "[P]rotected health information … may not necessarily include diagnosis-specific information, such as information about the treatment of an individual, and may be limited to demographic or other information not indicative of the type of health care services provided to an individual. If the information is tied to a covered entity, then it is protected health information since it is indicative that the individual received health care services or benefits from the covered entity, and therefore it must be protected … in accordance with the HIPAA rules.").

70. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care… Patient privacy encompasses a number of aspects, including, … personal data (informational privacy)[.]

71. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

72. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must: (c) Release patient information only in keeping ethics guidelines for confidentiality.[32]

73. MiniMed's use of Tracking Tools also violates Federal Trade Commission ("FTC") data security guidelines, and the agency has promulgated several business guides that highlight the importance of implementing reasonable data security practices.

74. The FTC's October 2016 publication *Protecting Personal Information: A*

---

[32] AMA Principles of Medical Ethics: I, IV, *Chapter 3: Opinions on Privacy, Confidentiality & Medical Records*, https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf, American Medical Association (last visited Mar. 21, 2023).

Guide for Business[33] established cyber-security guidelines for businesses, stating businesses must protect personal patient information; properly dispose of it when it is no longer needed; encrypt information stored on computer networks; understand network vulnerabilities; and implement policies to correct any security problems.

75. Upon information and good faith belief, MiniMed failed to implement these basic, industry-wide data security practices.

Patients' Reasonable Expectation of Privacy.

76. Plaintiff and Class Members were aware of MiniMed's duty of confidentiality when they sought medical services from MiniMed.

77. Indeed, every time Plaintiff and Class Members provided their PII and PHI to MiniMed, they each had a reasonable expectation that the information would remain confidential, and that MiniMed would not share the Private Information with third parties for a commercial purpose or to any third-party marketing company.

78. Privacy polls and studies show that most Americans consider obtaining an individual's affirmative consent before a company collects and shares its customers' data to be one of the most important privacy rights.

79. For example, a recent Consumer Reports study shows that 92% of Americans believe internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.[34]

---

[33] Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 2, 2023).

[34] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/, CONSUMERREPORTS.ORG (last visited Jun. 2, 2023).

80. Personal data privacy and obtaining consent to share Private Information are material to Plaintiff and Class Members.

IP Addresses are Protected Health Information.

81. Based on information and belief, MiniMed improperly disclosed Plaintiff's and Class Members' computer IP addresses to third parties like Google *in addition to* names, phone numbers, email addresses, dates of birth, unique MiniMed client ID numbers, patient statuses, medical conditions, treatments, and readings.

82. An IP address is a number that identifies the address of a device connected to the Internet, and it is used to identify and route communications on the Internet, they individuals' IP addresses are used by Internet service providers, websites, and third-party tracking companies to facilitate and track communications.

83. Google tracks every IP address ever associated with a Google user, and uses it to target individual homes and their occupants with advertising.

84. Under HIPAA, an IP address is considered personally identifiable information, defining personally identifiable information as including "any unique identifying number, characteristic or code" and specifically listing IP addresses among examples. 45 C.F.R. § 164.514 (2).

85. HIPAA further declares information as personally identifiable where the covered entity has "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. § 164.514(2)(ii); *see also*, 45 C.F.R. § 164.514(b)(2)(i)(O). Here, MiniMed knew or should have known of the risks posed by the Tracking Technologies it used, and it should have been aware of the particular risk posed to individuals with Google accounts.

86. Consequently, MiniMed's disclosure of Plaintiff's and Class Members' IP addresses violated HIPAA and industry-wide privacy standards.

MiniMed was Enriched and Benefitted from its Use of the Tracking Tools and Unauthorized Disclosures

87. The primary motivation and a determining factor in MiniMed's interception and disclosure of Plaintiff's and Class Members' Private Information was to commit criminal and tortious acts in violation of federal and state laws as alleged herein, namely, the unauthorized use of patient data for advertising in the absence of express written consent. MiniMed's specifically undertook this course of conduct, with regard to both marketing and revenue generation, in violation of HIPAA, common law privacy rights, and its own stated policies.

88. In exchange for disclosing its Patients' PII to Google and other third-parties, MiniMed was compensated in the form of enhanced advertising services and more cost-efficient marketing on Google.

89. Based on information and belief, MiniMed was advertising its services on Google and other third-party advertisers' websites, including by retargeting patients and potential patients via online advertisements.

Class Members' Data Had Financial Value

90. Moreover, Plaintiff's and Class Members' Private Information had value and MiniMed's disclosure and interception harmed Plaintiff and the Class.

91. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is expected to continue increasing, and projected estimates for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.

92. In addition, Google itself has implemented a pilot program in which it pays users $3.00 per week to track them.

93. The value of health data is well-known and has been reported extensively in the media. For example, a 2017 article by Time Magazine titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" describes the extensive market for health

data, noting it is both lucrative and a significant risk to privacy.[35]

94. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[36]

95. Several companies have products through which they pay consumers for a license to track certain information. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for browsing history information.

96. Tech companies are under scrutiny because they already have access to a massive trove of information about people, which they use to serve their own purposes, including potentially micro-targeting advertisements to people with certain health conditions.

97. Policymakers are proactively calling for a revision and potential upgrade of the HIPAA privacy rules out of concern for what might happen as tech companies continue to march into the medical sector.[37]

98. Private Information is also a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use Private Information to commit an array of crimes that include identity theft and medical and financial fraud.[38] A robust "cyber black market" exists where criminals openly post stolen PII and PHI on multiple underground Internet websites, commonly referred to as the dark web.

99. While credit card information and associated IIHI can sell for as little as $1–

---

[35] *See* https://time.com/4588104/medical-data-industry/ (last visited June 7, 2023).

[36] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited June 7, 2023).

[37] *Id.*

[38] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Mar. 16, 2023).

$2 on the black market, PHI can sell for as much as $363.[39] PHI is particularly valuable because criminals can use it to target victims with frauds that take advantage of their medical conditions. PHI can also be used to create fraudulent insurance claims, facilitate the purchase and resale of medical equipment, and gain access to prescriptions for illegal use or sale. Medical identity theft can result in inaccuracies in medical records, costly false claims, and even life-threatening consequences.

100. The FBI Cyber Division issued a Private Industry Notification on April 8, 2014, that advised the following:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.

101. Cybercriminals often trade stolen Private Information on the black market for years following a breach or disclosure. Stolen Private Information can be posted on the Internet, making it publicly available.

102. MiniMed gave away Plaintiff's and Class Members' communications and transactions on its Digital Platforms without permission.

103. The unauthorized access to Plaintiff's and Class Members' private and Personal Information has diminished the value of that information, resulting in harm to Website and App Users, including Plaintiff and Class Members.

PLAINTIFF'S EXPERIENCES

Plaintiff A.H.

104. Plaintiff has used MiniMed's InPen App and services from MiniMed since

---

[39] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at*: https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last accessed Mar. 16, 2023).

approximately July of 2020 and accessed those services through the Digital Platforms.

105. Plaintiff used Google's services during the relevant period because he has a Google email account ("Gmail"), which he has used on one or more of the same devices that he used to access the Digital Platforms. Based on the foregoing, and upon information and belief, Google knows Plaintiff's real identity, and it can identify him based on additional data points such as his device identifiers.

106. Plaintiff's specific therapy settings for the InPen were provided to him through his healthcare provider.

107. Plaintiff met with an InPen Representative who walked him through the process of inputting his specified therapy settings into the InPen System and App.

108. Plaintiff used the App to log his meals and carb intake, and in turn, it would then instruct him to test his blood sugar through his CGM. The App calculated his insulin dosage based on his current blood sugar, last reported meal, and his unique therapy settings as provided by his physician. Plaintiff relied on the App for these calculations, and he would subsequently inject himself with the specified insulin dosage. He repeated this process, using the App after every meal, and communicated information and received subsequent calculations several times each day.

109. The InPen system allowed Plaintiff to link external accounts to the InPen App and system, including but not limited to Dexcom, and Dexcom6, in conjunction with his treatment and in order to better manage his diabetes. Likewise, the InPen system worked seamlessly with his healthcare provider.

110. In April 2023, Plaintiff A.H. received a notification from MiniMed informing him that his Private Information was shared with third parties, including Google, without his consent.

111. As a direct and proximate result of MiniMed's conduct, Google was permitted to surreptitiously access his PII and PHI in relation to a medical device he wears and relies upon each day, and the InPen App, which he relied on each day.

112. The precise information transmitted and disclosed to Google is within the

exclusive control of MiniMed and/or third parties who received it, including but not limited to Google; however, upon information and belief, Google and other third parties received data and information revealing Plaintiff's name, phone number, email address, date of birth, IP address, MiniMed unique client ID numbers, testing and reading information, device identifiers, and other sensitive medical information.

113. Plaintiff reasonably expected that his communications with MiniMed were confidential and private, and that such communications would remain confidential. Under no circumstance did he expect or anticipate that his confidential and protected Private Information would be transmitted to and/or intercepted by Google and other third parties.

114. To the contrary, Plaintiff provided his Private Information to MiniMed with the expectation and trust that the information would remain confidential and protected according to state and federal law.

115. Had MiniMed disclosed its surreptitious duplication, transmission, interception, and assistance with intercepting Private Information, Plaintiff would not have obtained MiniMed's services (or at minimum would have paid less) and would not have provided MiniMed with his Private Information. And had MiniMed's conduct been adequately disclosed, Plaintiff would have been aware of it.

116. Plaintiff has suffered injuries as a result of MiniMed's conduct, including (i) invasion of privacy, (ii) loss of benefit of the bargain, (iii) diminution of value of Private Information, (iv) breach of implied contract, and the continued and ongoing risk to his Private Information, including the improper use of his medical diagnosis.

TOLLING

117. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiff did not know (and had no way of knowing) that his Private Information was intercepted and unlawfully disclosed because MiniMed did not disclose this information until on or about April 2023. Plaintiff first learned of MiniMed's conduct after receiving the Notice letter described herein.

CLASS ACTION ALLEGATIONS

118. This is a class action pursuant to Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedures on behalf of the following Classes:

- Nationwide Class - All MiniMed Patients who used MiniMed's Digital Platforms and InPen while residing in the United States.

- New York Subclass - All MiniMed Patients who are residents of the State of New York.

119. Excluded from the Class and the Subclass are Defendants, their respective agents, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any MiniMed's officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

120. Plaintiff reserves the right to modify or to amend the definition of the proposed classes before the Court determines whether certification is appropriate.

121. Numerosity, Fed R. Civ. P. 23(a)(1). Each of the Classes consists of thousands of individuals. Accordingly, members of the Classes are so numerous that joinder of all members is impracticable. Class members may be identified from MiniMed's records.

122. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3). Questions of law and fact common to each Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent MiniMed had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether MiniMed had a duty to ensure Plaintiff and Class Members' Private Information was not to disclosed to unauthorized third parties;

c. Whether MiniMed violated its Privacy Policies by disclosing the Private Information of Plaintiff and Class Members to Google and/or additional third parties;

d. Whether MiniMed adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information was disclosed to third parties and continues to be disclosed to third-parties;

e. Whether MiniMed violated the law by failing to obtain patient consent prior to disclosures described herein;

f. Whether MiniMed adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;

g. Whether MiniMed acted knowingly and purposely when it installed and implemented Tracking Tools based on, amongst other things, its statements and representations concerning the value of patient data;

h. Whether MiniMed engaged in unfair, unlawful, or deceptive practices by outfitting its Web Properties with Tracking Tools;

i. Whether MiniMed violated the consumer protection statutes invoked herein;

j. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of MiniMed wrongful conduct;

k. Whether MiniMed knowingly made false representations as to its data sharing practices and/or Privacy Policy practices;

l. Whether MiniMed knowingly omitted material representations with respect to its data sharing practices and/or Privacy Policies practices;

m. Whether MiniMed's knowing disclosure of its patients' individually identifiable health information to Google or other third parties are "criminal or tortious" under 18 U.S.C § 2511(2)(d); and

n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm they face as a result of the disclosure of their Private Information.

123. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of the claims of other Class members, as all members of the Classes were uniformly affected by MiniMed's wrongful conduct in violation of federal and state law.

124. Adequacy, Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of Class Members in that Plaintiff have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

125. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3). Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit many Class Members to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation, like MiniMed. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

126. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because MiniMed would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course

of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

127. The litigation of the claims brought herein is manageable. MiniMed's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

128. Based on information and belief, adequate and direct notice can be given to Class Members using information maintained in MiniMed's records.

129. Unless a Class-wide injunction is issued, MiniMed may continue in its failure to properly secure the Private Information of Class Members, MiniMed may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and it may continue to act unlawfully as set forth in this Complaint.

130. Further, MiniMed has acted or refused to act on grounds generally applicable to each Class and, accordingly, final injunctive or corresponding declaratory relief regarding Class Members is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

131. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether MiniMed owed a legal duty to not disclose Plaintiff's and Class Members' Private Information;

b. Whether MiniMed owed a legal duty to not disclose Plaintiff's and Class Members' Private Information with respect to MiniMed's Privacy Policies;

c. Whether MiniMed breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

d. Whether MiniMed failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

e. Whether MiniMed adequately and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;

f. Whether MiniMed failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties; and

g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief because of MiniMed's wrongful conduct.

CALIFORNIA LAW SHOULD APPLY TO PLAINTIFF'S & CLASS MEMBERS' COMMON LAW CLAIMS

132. The State of California has a significant interest in regulating the conduct of businesses operating within its borders.

133. California, which seeks to protect the rights and interests of California and all residents and citizens of the United States against a company headquartered and doing business in California, has a greater interest in the claims of Plaintiff and the Classes than any other state and is most intimately concerned with the claims and outcome of this litigation.

134. The principal place of business and headquarters of MiniMed, located in Northridge, California, is the "nerve center" of its business activities—the place where its high-level officers direct, control and coordinate its activities, including major policy, financial, and legal decisions.

135. Upon information and good faith belief, MiniMed's actions and corporate decisions surrounding the allegations made in the Complaint were made from and in California.

136. MiniMed's breaches of duty to Plaintiff and Class Members emanated from California.

137. Application of California law to the Classes with respect to Plaintiff's and

the Classes' common law claims is neither arbitrary nor fundamentally unfair because choice of law principles applicable to this action support the application of the common law of California to the nationwide common law claims of all Class members.

138. Additionally, given California's significant interest in regulating the conduct of businesses operating within its borders, and that California has the most significant relationship to MiniMed because it is headquartered in California, there is no conflict in applying California law to non-resident consumers such as Plaintiff and Class members.

139. Alternatively, and/or in addition to California law, the common law claims are brought under the laws of the states in which each named Plaintiff resides.

CLAIMS FOR RELIEF

COUNT I
Common Law Invasion of Privacy – Intrusion Upon Seclusion
(*On Behalf of Plaintiff and the Nationwide Class*)

140. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

141. Plaintiff and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications and protected health information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to wiretaps without Plaintiff's and Class Members' knowledge or consent.

142. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with MiniMed via its Digital Platforms and the communications platforms and services therein.

143. Plaintiff and Class Members communicated sensitive PII that they intended for only MiniMed to receive and based on their understanding that it would be kept private and secure, and not transmitted or intercepted by Google at MiniMed's behest.

144. MiniMed's disclosure of the substance and nature of those communications

to third parties without the knowledge and consent of Plaintiff and Class members is an intentional intrusion on Plaintiff's and Class members' solitude or seclusion.

145. Plaintiff and Class Members had a reasonable expectation of privacy because MiniMed is a HIPAA covered entity that provided Plaintiff and Class Members with medical devices and products and services specifically related to their health conditions and treatment.

146. Moreover, Plaintiff and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential.

147. MiniMed's disclosure of private medical information coupled with individually identifying information is highly offensive to the reasonable person.

148. As a result of MiniMed's actions, Plaintiff and Class Members have suffered harm and injury including, but not limited to, an invasion of their privacy rights.

149. Plaintiff and Class Members have been damaged as a direct and proximate result of MiniMed's invasion of their privacy and are entitled to compensatory and/or nominal damages.

150. Plaintiff and Class Members seek appropriate relief for that injury including, but not limited to, damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as a result of the intrusions upon their privacy.

151. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of MiniMed's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter MiniMed from engaging in such conduct in the future.

152. Plaintiff also seeks such other relief as the Court may deem just and proper.

COUNT II
Breach of Confidence
(*On Behalf of Plaintiff and the Nationwide Class*)

153. Plaintiff repeats the allegations contained in the foregoing paragraphs as if

fully set forth herein.

154. Medical providers have a duty to their patients to keep non-public medical information completely confidential.

155. Plaintiff and Class Members had a reasonable expectation of privacy in: (1) their use of MiniMed's Web Properties—such as when they used the InPen app to calculate doses and record other information; (2) all communications made via MiniMed's Web Properties; and (3) the PII and PHI they shared with MiniMed.

156. Plaintiff's and Class Members' reasonable expectations of privacy were based on MiniMed's status as a healthcare provider and further buttressed by MiniMed's express promises in its Privacy Policies.

157. Contrary to its duties as a medical provider and its express promises of confidentiality, MiniMed intentionally deployed Tracking Tools that disclosed and transmitted Plaintiff's and Class Members' Private Information, communications made via MiniMed's Web Platforms, and the contents of their communications exchanged with MiniMed to third parties.

158. The third-party recipients included but were not limited to Google and other online marketers.

159. MiniMed's disclosures of Plaintiff's and Class Members' Private Information were made without their knowledge, consent, or authorization, and were unprivileged.

160. The harm arising from a breach of confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

161. As a direct and proximate cause of MiniMed's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiff and Class Members were damaged by MiniMed's breach in that:

a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;

b. MiniMed eroded the essential confidential nature of the provider-patient

relationship;

c. MiniMed took something of value from Plaintiff and Class Members and derived benefit therefrom without their knowledge or informed consent and without compensating them for the data;

d. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included MiniMed's duty to maintain confidentiality;

e. MiniMed's actions diminished the value of Plaintiff's and Class Members' Private Information and

f. MiniMed's actions violated the property rights Plaintiff and Class Members have in their Private Information.

162. Plaintiff and Class Members are therefore entitled to general damages for invasion of their rights in an amount to be determined by a jury and nominal damages for each independent violation. Plaintiff is also entitled to punitive damages.

COUNT III
Breach of Fiduciary Duty
(*On behalf of Plaintiff & the Nationwide Class*)

163. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

164. In light of the special relationship between MiniMed and Plaintiff and Class Members, whereby MiniMed became guardian of Plaintiff's and Class Members' Private Information, it became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of an unauthorized disclosure; and (3) to maintain complete and accurate records of what information (and where) MiniMed did and does store.

165. MiniMed has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of MiniMed's relationship with its patients and

former patients to keep secure their Private Information.

166. MiniMed breached its fiduciary duties to Plaintiff and Class Members by disclosing their Private Information to unauthorized third parties, and separately, by failing to notify Plaintiff and Class Members of this fact.

167. As a direct and proximate result of MiniMed's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer injury and are entitled to compensatory, nominal, and/or punitive damages, and disgorgement of profits, in an amount to be proven at trial.

COUNT IV
Negligence
(*On behalf of Plaintiff & the Nationwide Class*)

168. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

169. MiniMed required Plaintiff and Class Members to submit non-public personal information to obtain healthcare/medical services.

170. By collecting and storing this data, MiniMed had a duty of care to use reasonable means to secure and safeguard its Digital Platforms and servers—and Class Members' Private Information held within them—to prevent disclosures and safeguard the Private Information from disclosure to third parties.

171. MiniMed's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

172. MiniMed owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

173. MiniMed's duty of care to use reasonable security measures arose because of the special relationship between MiniMed and InPen users, which is recognized by

laws and regulations including but not limited to HIPAA, as well as common law.

174. MiniMed was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

175. MiniMed's duty to use reasonable security measures under HIPAA required MiniMed to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

176. In addition, MiniMed had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

177. MiniMed's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because it is bound by industry standards to protect confidential Private Information.

178. MiniMed breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions committed include, but are not limited to:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Plaintiff's and Class Members' Private Information;

d. Failing to detect in a timely manner that Plaintiff's and Class Members' Private Information had been compromised; and

e. Failing to timely notify Plaintiff and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

179. It was foreseeable that MiniMed's failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and Class Members.

180. Plaintiff and Class Members are entitled to compensatory, nominal, and/or punitive damages.

181. MiniMed's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner. Therefore, Plaintiff and Class Members are also entitled to injunctive relief requiring MiniMed to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT V
Breach of Implied Contract
(*On Behalf of Plaintiff & the Nationwide Class*)

182. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

183. When Plaintiff and Class Members provided Private Information to MiniMed in exchange for medical services, they entered an implied contract based on Minimed's status as a healthcare provider pursuant to which MiniMed agreed to safeguard and not disclose Plaintiff's and Class Members' Private Information without first obtaining proper consent.

184. Plaintiff and Class Members accepted MiniMed's offers and provided their Private Information to MiniMed.

185. Plaintiff and Class Members would not have entrusted MiniMed with their Private Information in the absence of an implied contract between them and Minimed's

obligation to not disclose Private Information without patient consent.

186. MiniMed breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information to third parties like Google.

187. As a direct and proximate result of MiniMed's breach of these implied contracts, Plaintiff and Class Members sustained damages as alleged herein.

188. Plaintiff and Class Members would not have used MiniMed's services or would have paid substantially for them, had they known their Private Information would be disclosed to Google.

189. Plaintiff and Class Members are entitled to compensatory, consequential, and/or nominal damages because of MiniMed's breaches of implied contract.

COUNT VI
Breach of Implied Covenant of Good Faith and Fair Dealing
(*On Behalf of Plaintiff & the Nationwide Class*)

190. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

191. Plaintiff and Class Members entered valid, binding, and enforceable implied contracts with MiniMed, as alleged above.

192. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts.

193. These included the implied covenants that MiniMed would act fairly and in good faith in carrying out its contractual obligations to take reasonable measures to protect Plaintiff's and Class Members' Private Information and to comply with industry standards and federal and state laws and regulations.

194. A "special relationship" exists between MiniMed and the Plaintiff and Class Members because InPen patients sought medical services from MiniMed and, in doing

so, entrusted MiniMed with their Private Information.

195. Despite this special relationship, MiniMed did not act in good faith and with fair dealing to protect Plaintiff's and Class Members' Private Information.

196. Plaintiff and Class Members performed all conditions, covenants, obligations, and promises owed to MiniMed.

197. MiniMed's failure to act in good faith in implementing the security measures required by the contracts denied Plaintiff and Class Members the full benefit of their bargain, and instead they received healthcare and related services that were less valuable than what they paid for and less valuable than their reasonable expectations under the contracts. Plaintiff and Class Members were damaged in an amount at least equal to this overpayment.

198. MiniMed's failure to act in good faith in implementing the security measures required by the contracts also caused Plaintiff and Class Members to suffer actual damages resulting from the disclosure and interception of their Private Information and they remain at imminent risk of suffering additional damages in the future.

199. Accordingly, Plaintiff and Class Members have been injured because of MiniMed's breach of the covenant of good faith and fair dealing and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT VII
Unjust Enrichment/Restitution
(*On behalf of Plaintiff & the Nationwide Class*)

200. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

201. Upon information and belief, MiniMed funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

202. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount

of the portion of each payment made that is allocated to data security is known to MiniMed.

203. Plaintiff and Class Members conferred a monetary benefit on MiniMed. Specifically, they purchased goods and services from MiniMed and/or its agents and in so doing provided MiniMed with their Private Information.

204. In exchange, Plaintiff and Class Members should have received goods and services that did not compromise their Private Information or cause its transfer to unintended third-parties such as Google—i.e. they expected MiniMed to put systems in place to protect their Private Information with adequate data security.

205. MiniMed knew that Plaintiff and Class Members conferred a benefit, it accepted and profited from these transactions, and its used InPen users' Private Information to its own benefit for business and marketing purposes to increase its profits.

206. MiniMed enriched itself by obtaining the inherent value of Plaintiff's and Class Members' Private Information, sharing it with third-parties (and/or aiding in its interception), and saving costs it reasonably should have expended on marketing and/or data security measures to secure the Private Information.

207. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of MiniMed's decision to prioritize its profits over requisite security.

208. Under the principles of equity and good conscience, MiniMed should not be permitted to retain the money belonging to Plaintiff and Class Members, because MiniMed failed to implement appropriate data management and security measures that are mandated by industry standards.

209. MiniMed failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

210. If Plaintiff and Class Members had been aware of MiniMed's data sharing practices, they would not have agreed to provide their Private Information to MiniMed or use its Digital Platforms.

211. Plaintiff and Class Members have no adequate remedy at law for this count. An unjust enrichment theory provides the equitable disgorgement of profits even where an individual has not suffered a corresponding loss in the form of money damage.

212. Furthermore, California law permits a standalone claim for unjust enrichment, allowing the court to construe the cause of action as a quasi-contract claim. *E.g., Astiana v. Hain Celestial Group, Inc*., 783 F.3d 753, 756 (9th Cir. 2015). California law recognizes a right to disgorgement of profits resulting from unjust enrichment, even where an individual has not suffered a corresponding loss. *In re Facebook, Inc. Internet Tracking Litig*., 956 F.3d 589, 599 (9th Cir. 2020). California law requires disgorgement of unjustly earned profits regardless of whether a MiniMed's actions caused a plaintiff to directly expend his or her own financial resources or whether a MiniMed's actions directly caused the plaintiff's property to become less valuable. Under California law, a stake in unjustly earned profits exists regardless of whether an individual planned to sell his or her data or whether the individual's data is made less valuable.

213. As a direct and proximate result of MiniMed's conduct, Plaintiff and Class Members have suffered and will continue to suffer injury.

214. MiniMed should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them, or to refund the amounts that Plaintiff and Class Members overpaid for its services.

COUNT VIII
Violations of Electronic Communications Privacy Act ("ECPA")
18 U.S.C. § 2511(1), *et seq*.
Unauthorized Interception, Use, and Disclosure
(On Behalf of Plaintiff and the Nationwide Class)

215. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

216. The ECPA protects both sending and receipt of communications.

217. 18 U.S.C. § 2520(a) provides a private right of action to any person whose

wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

218. The transmissions of Plaintiff's PII and PHI to MiniMed's Digital Platforms in conjunction with wearable devices qualifies as "communications" under the ECPA's definition of 18 U.S.C. § 2510(12).

219. Electronic Communications. The transmission of PII and PHI between Plaintiff and Class Members and MiniMed's Digital Platforms with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo optical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

220. Content. The ECPA defines content, when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

221. Interception. The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

222. Electronical, Mechanical or Other Device. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiff's and Class Members' browsers;

b. Plaintiff's and Class Members' computing devices;

c. Plaintiff's and Class Members' wearable devices;

d. MiniMed's webservers and Digital Platforms;

e. The Tracking Tools deployed by MiniMed to effectuate the sending and

acquisition of patient communications.

223. By utilizing and embedding Tracking Tools on its Digital Platforms, MiniMed intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

224. Specifically, MiniMed intercepted Plaintiff's and Class Members' electronic communications via the Tracking Tools, which tracked, stored, and unlawfully disclosed their Private Information to Google.

225. The intercepted communications include, but are not limited to, communications to/from Plaintiff and Class Members regarding PII and PHI, treatment, medication, and scheduling.

226. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), MiniMed violated 18 U.S.C. § 2511(1)(c).

227. By intentionally using, or endeavoring to use, the contents of the electronic communications of InPen users, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), MiniMed violated 18 U.S.C. § 2511(1)(d).

228. Unauthorized Purpose. MiniMed intentionally intercepted the contents of InPen users' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State—namely, invasion of privacy, among others.

229. The ECPA provides that a "party to the communication" may be liable where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C § 2511(2)(d).

230. MiniMed is not a party to the communications based on its unauthorized duplication and transmission of InPen users' communications, which are material and were not disclosed to Plaintiff and Class Members—i.e. they exceed the scope of any purported consent. Thus, even if MiniMed is a party to InPen users' communications, its simultaneous, unknown duplication, forwarding, and interception of Plaintiff's and Class members' Private Information does not qualify for the party exemption.

231. MiniMed's acquisition of patient communications, which were used and disclosed to Google, was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and individual States nationwide as set forth herein, including:

a. Criminal violation of HIPAA, 42 U.S.C. § 1320d-6;

b. Invasion of privacy;

c. Breach of confidence;

d. Breach of fiduciary duty;

e. California Invasion of Privacy Act, §§ 630, et. seq.;

f. California Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56, *et seq*.;

g. Violation of NY Gen. Bus. Law §349 *et seq*.

232. MiniMed's conduct violated 42 U.S.C. § 1320d-6 in that they: used Tracking Tools without patient authorization; the Tracking Tools were provided by Google, which individually identifies people across the United States—including InPen users—based on device ids and related information; and caused the unauthorized disclosure of individually identifiable health information to Google without patient authorization.

233. The penalty for violation is enhanced where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6.

234. MiniMed's conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because MiniMed's use of Google source code was for MiniMed's

commercial advantage to increase revenue from existing patients and gain new patients.

235. MiniMed is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) as a participant in Plaintiff's and Class Members' communications via the Digital Platforms because MiniMed used any purported participation in these communications to improperly share Private Information with Google, who did not participate in these communications and was not authorized or permitted to receive this information.

236. Simply put, MiniMed cannot viably claim any exception to ECPA liability.

237. Plaintiff and Class members have suffered damages as a direct and proximate result of MiniMed's invasion of privacy in that:

a. Learning that MiniMed has intruded upon, intercepted, transmitted, shared, and used their PII and PHI for commercial purposes has caused Plaintiff and the Class members to suffer emotional distress;

b. MiniMed received substantial financial benefits from its use of Plaintiff's and the Class members' PII and PHI without providing any value or benefit to Plaintiff or the Class members;

c. MiniMed received substantial, quantifiable value from its use of Plaintiff's and the Class members' PII and PHI, such as understanding how people use its web properties and determining what ads people see on its web properties, without providing any value or benefit to Plaintiff or the Class members;

d. MiniMed failed to provide Plaintiff and the Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information; and

e. The diminution in value of Plaintiff's and Class Members' PII and PHI and the loss of privacy due to MiniMed's disclosure of sensitive and confidential information that Plaintiff and Class Members intended to remain private.

238. MiniMed intentionally used the wire or electronic communications to avoid HIPAA regulations and industry standards, all to increase its profit margins, and specifically used Tracking Tools to monetize Plaintiff's and Class Members' Private

Information for its own financial gain, and to their detriment.

239. MiniMed was not acting under color of law to intercept Plaintiff's and the Class Members' wire or electronic communication.

240. Plaintiff and Class Members did not authorize MiniMed to acquire the content of their communications for the purposes described herein.

241. Any purported consent Medtronic received from Plaintiff and Class Members was not valid.

242. In sending and in acquiring the content of Plaintiff's and Class Members' information, MiniMed's purpose was tortious, criminal, and designed to violate federal and state legal provisions including a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person.

243. As a result of MiniMed's violation of the ECPA, Plaintiff and the Class are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT IX
Violations of The ECPA
18 U.S.C. § 2511(3)(a), *et seq*.
Unauthorized Divulgence by Electronic Communications Service
(*On Behalf of Plaintiff & the Nationwide Class*)

244. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

245. The ECPA provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

246. Electronic Communication Service. An "electronic communication service"

is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

247. MiniMed's Digital Platforms are an electronic communication service. The App and Website provide to users thereof the ability to send or receive electronic communications. In the absence of MiniMed's Digital Platforms, internet users could not send or receive communications regarding Plaintiff's and Class Members' PII and PHI.

248. Intentional Divulgence. MiniMed intentionally used the Tracking Technology to and was aware, or should have been aware, that doing so would result in the divulgence of Plaintiff's and Class Members' PII and PHI.

249. While in Transmission. Upon information and belief, MiniMed's divulgence of the contents of Plaintiff's and Class Members' communications was contemporaneous with their exchange with MiniMed's Digital Platforms.

250. MiniMed divulged the contents of Plaintiff's and Class Members' electronic communications to third parties like Google without authorization.

251. Exceptions do not apply. In addition to the exception for communications directly to an ECS or an agent of an ECS, the Wiretap Act states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication as follows:

a. "as otherwise authorized in section 2511(2)(a) or 2517 of this title;"

b. "with the lawful consent of the originator or any addressee or intended recipient of such communication;"

c. "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;" or,

d. "which were inadvertently obtained by the service provider, and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency." 18 U.S.C. § 2511(3)(b).

252. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

253. MiniMed's divulgence of the contents of Plaintiff's and Class Members' communications on MiniMed's Digital Platform was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of MiniMed's service; nor (2) necessary to the protection of the rights or property of MiniMed.

254. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

255. MiniMed's divulgence of the contents of user communications was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above: (a) Plaintiff and Class Members did not authorize MiniMed to divulge the contents of their communications; and (b) MiniMed did not procure the "lawful consent" from the Digital Platforms with which Plaintiff and Class Members were exchanging information.

256. Moreover, MiniMed divulged the contents of Plaintiff's and Class Members' communications and Private Information through to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

257. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Medtronic did not divulge the contents

of their communications to a law enforcement agency.

258. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and reasonable attorney fees and other litigation costs reasonably incurred.

COUNT X
Violation of Title II of the Electronic Communications Privacy Act
18 U.S.C. § 2702, *et seq*.
The Stored Communications Act ("SCA")
(On Behalf of Plaintiff and the National Class)

259. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

260. The ECPA provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

261. Electronic Communication Service. ECPA defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

262. MiniMed's InPen App qualifies as an Electronic Communication Service because it was specifically designed to work as a conduit of communication between Plaintiff and Class Members and their respective medical providers, including MiniMed.

263. MiniMed intentionally procures and embeds various Tracking Tools on its Digital Platforms to intercept InPen user's communications.

264. Electronic Storage. ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

265. When Plaintiff or Class Member communicates with the Digital Platform, through their insulin tracking and dosage the content of that communication is immediately placed into storage.

266. MiniMed knowingly divulges the contents of Plaintiff's and Class Members' communications through its Digital Platform's source code.

267. Exceptions Do Not Apply. Section 2702(b) of the Stored Communication Act provides that an electronic communication service provider "may divulge the contents of a communication—"

a. "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient."

b. "as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this title;"

c. "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;"

d. "to a person employed or authorized or whose facilities are used to forward such communication to its destination;"

e. "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;"

f. "to the National Center for Missing and Exploited Children, in connection with a reported submission thereto under section 2258A."

g. "to law enforcement agency, if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime;"

h. "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency"; or

i. "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies Section 2523."

268. MiniMed did not divulge the contents of Plaintiff's and Class Members' communications to "addressees," "intended recipients," or "agents" of any such addressees or intended recipients of Plaintiff and Class Members.

269. Section 2517 and 2703 of the ECPA relate to investigations by government officials and have no relevance here.

270. Section 2511(2)(a)(i) provides:

"It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks."

271. MiniMed's divulgence of the contents of Plaintiff's and Class Members' communications to Google was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of MiniMed's services; nor (2) necessary to the protection of the rights or property of MiniMed.

272. MiniMed's divulgence of the contents of user communications was not done

"with the lawful consent of the originator or any addresses or intend recipient of such communication[s]." As alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from the Digital Platform or App with which Plaintiff and Class Members were exchanging information.

273. Moreover, MiniMed divulged the contents of Plaintiff's and Class Members' communications to Google, who is not a "person[s] employed or whose facilities are used to forward such communication to its destination."

274. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and MiniMed did not divulge the contents of their communications to a law enforcement agency.

275. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages if applicable in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT X

Violations of Cal. Penal Code §630, *et seq.*
California Invasion of Privacy Act ("CIPA")
(On Behalf of Plaintiff & the Nationwide Class)

276. Plaintiff repeats the allegations above as if fully set forth herein and brings this count individually and on behalf of himself and the Nationwide Class.

277. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose.

> The Legislature thereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques

> has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

California Penal Code § 631(a) provides, in pertinent part (emphasis added):

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner … willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or **who aids, agrees with, employs, or conspires** with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500).

278. Under CIPA, a defendant must show it had the consent of all parties to a communication, and consent is not an all or nothing proposition.

279. At all relevant times, MiniMed aided, employed, agreed with, and conspired with Google to track and intercept Plaintiff's and Class Members' communications via its Digital Platforms. These communications were transmitted to and intercepted by a third party during the communication and without the knowledge, authorization, or consent of Plaintiff and Class Members.

280. MiniMed intentionally inserted an electronic listening device onto Plaintiff's and Class Members' mobile devices and, without their knowledge or consent,

tracked and transmitted the substance of their confidential communications to Google for marketing purposes.

281. MiniMed willingly facilitated Google's interception and collection of Plaintiff's and Class Members' private medical information by embedding Tracking Tools into the App. MiniMed had full control over its use and implementation of the tool, and Google would not have received InPen users' Private Information but for MiniMed's conduct and decision to monetize InPen users' data.

282. The Tracking Tools MiniMed used constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, these tools fall under the broad catch-all category of "any other manner."

283. MiniMed failed to disclose its use of Google Analytics to InPen patients.

284. The Tracking Tools are designed to intercept InPen users' communications contemporaneously as patients use the App, and the communications were intercepted in transit, before arriving at their final destination.

285. As demonstrated hereinabove, MiniMed violated CIPA by aiding and permitting Google to intercept and receive InPen Users' communications in real time through its Digital Platforms.

286. By disclosing Plaintiff's and Class Members' Private Information, MiniMed violated Plaintiff's and Class Members statutorily protected right to privacy.

287. Thus, pursuant to CIPA Section 637.2, MiniMed is liable to Plaintiff and Class Members for treble actual damages related to their loss of privacy in an amount to

be determined at trial or for statutory damages in the amount of $5,000 per violation. Section 637.2 specifically states, "[it] is not a necessary prerequisite to an action pursuant to this section that the Plaintiff has suffered, or be threatened with, actual damages."

288. Under the statute, MiniMed is also liable for reasonable attorney's fees, litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by MiniMed in the future.

COUNT XII
Violation of New York General Business Law § 349
(On behalf of Plaintiff and the New York Subclass)

289. Plaintiff and New York Subclass repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

290. This cause of action is brought pursuant to the New York General Business Law § 349 ("NYGBL"), which New York courts have invariably interpreted using the kind of liberal construction afforded to state consumer protection statutes intended to prevent fraud.

291. NYGBL § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

292. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of NYGBL § 349 because its act of implementing Tracking Tools and sharing patient data is a "business practice" within the meaning of NYGBL § 349, and the deception occurred within New York State where Plaintiff resides.

293. By serving as Plaintiff's and Class Members' healthcare provider, Defendant had a duty to protect their Private Information from unlawful disclosure.

294. Plaintiff and the Class Members paid for or otherwise availed themselves and received services from Defendant, for the purpose of medical treatment.

295. Defendant engaged in the conduct alleged in this Class Action Complaint, entering transactions intended to result, and which did result, in the provision of medical treatment to Plaintiff and Class Members.

296. Defendant's acts, practices, and omissions were done during Defendant's offer of medical treatment, services, and care throughout the state of New York and the United States.

297. Defendant, operating in and out of New York, engaged in unfair, unconscionable, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of NYGBL § 349, including but not limited to the following: (a) knowingly promising to protect Plaintiff's and Class Members' Private Information, (b) knowingly and improperly storing, possessing, using, and/or procuring the interception of, Plaintiff's and Class Members' Private Information; and (c) knowingly disclosing Plaintiff's and Class Members' Private Information to third parties, including Google.

298. Defendant committed these acts while concurrently representing that it would protect and not unlawfully disclose Plaintiff's and Class Members' Private Information as their healthcare provider.

299. These unfair, unconscionable, and unlawful acts and practices violated duties imposed by laws, including by not limited to HIPAA, the New York Patient's Bill of Rights, New York computer crime statutes, statutes regarding the confidentiality of medical records, and NYGBL § 349.

300. Defendant knew or should have known that its Digital Platform and the Tracking Tools thereon unlawfully wiretapped, intercepted, and disclosed Plaintiff's and Class Members' Private Information.

301. Plaintiff has standing to pursue this claim because as a direct and proximate result of Defendant's violations of NYGBL § 349, Plaintiff and Class Members have been "aggrieved" by a violation of NYGBL § 349 and bring this action to obtain a declaratory judgment that Defendant's acts or practices violate NYGBL § 349.

302. Plaintiff also has standing to pursue this claim because, as a direct result of

Defendant's knowing violation of NYGBL § 349, Plaintiff and Class Members have lost money or property in the form monies paid for Defendant's services, diminution in value of their Private Information, as well as loss of the benefit of their bargain with Defendant.

303. Plaintiff and Class Members are entitled to injunctive relief to protect them from the substantial and imminent risk of future loss of Private Information, including, but not limited to: (a) ordering that Defendant immediately remove any pixel, web beacon, cookie, or other tracking technology that causes the disclosure of Private Information to third parties without consent; (b) ordering that Defendant engage third-party security auditors and internal personnel to ensure Plaintiff's and Class Members' Private Information is no longer subject to the unlawful practices described in this Complaint; (c) ordering that Defendant purge, delete, and destroy Private Information not necessary for its provisions of services in a reasonably secure manner; (d) ordering that Defendant conduct regular database scans and security checks; (e) ordering Defendant to meaningfully educate individuals about the threats they face as a result of the loss of their Private Information to third parties and steps victims should take to protect themselves.

304. Plaintiff brings this action on behalf of himself and Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff, Class Members, and the public from Defendant's unfair methods of competition and unfair, unconscionable, and unlawful practices. Defendant's wrongful conduct as alleged in this Class Action Complaint has had widespread impact on the public at large.

305. The above unfair, unconscionable, and unlawful practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

306. Defendant's actions and inactions in engaging in the unfair, unconscionable, and unlawful practices described herein were negligent, knowing and willful, and/or

wanton and reckless.

307. Plaintiff and Class Members seek relief under NYGBL § 349, including, but not limited to, a declaratory judgment that its actions and/or practices violate NYGBL § 349; injunctive relief enjoining MiniMed from continuing to violate NYGBL § 349 as described above.

308. Plaintiff and Class Members are also entitled to recover actual damages, to recover the costs of this action (including reasonable attorneys' fees), and such other relief as the Court deems just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all members of the Classes defined herein, respectfully requests judgment against MiniMed and that the Court grant the following:

A. an Order certifying the Nationwide Class and appointing the respective Plaintiff and his Counsel to represent the Classes;

B. equitable relief enjoining MiniMed from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;

C. injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members;

D. an award of all damages available at equity or law, including, but not limited to, actual, consequential, punitive, and nominal damages, as allowed by law in an amount to be determined;

E. an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. pre- and post-judgment interest on all amounts awarded and

G. all such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the proposed Classes defined herein, respectfully demands a trial by jury for all claims asserted herein and so triable.

Date: August 30, 2023

Respectfully submitted,

/s/ *John Nelson*

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
jnelson@ milberg.com

Jonathan T. Deters*
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jdeters@msdlegal.com

Bryan L. Bleichner (SBN #220340)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
bbleichner@chesnutcambronne.com
pkrzeski@chesnutcambronne.com

Counsel for Plaintiff & Putative Classes

** Pro Hac Vice forthcoming*

ClassAction.org