| | |
|---|---|
| ASHIKA SINGH, *individually and on behalf of all others similarly situated*,<br><br>      Plaintiff,<br><br>v.<br><br>THE MOSES H. CONE MEMORIAL HOSPITAL OPERATING CORPORATION d/b/a CONE HEALTH and THE MOSES H. CONE MEMORIAL HOSPITAL d/b/a CONE HEALTH,<br><br>      Defendants. | Case No. 1:24-CV-558<br><br><br>**COMPLAINT – CLASS ACTION**<br><br><br>**JURY TRIAL DEMANDED** |

**CLASS ACTION COMPLAINT**

Plaintiff Ashika Singh ("Plaintiff"), a patient of The Moses H. Cone Memorial Hospital Operating Corporation d/b/a Cone Health and The Moses H. Cone Memorial Hospital d/b/a Cone Health  (together, "Cone Health" or "Defendants"), brings this class action lawsuit against Defendants individually and on behalf of all others similarly situated and alleges, upon personal knowledge as to her own actions and her counsel's investigation and—where indicated—upon information and good faith belief as to all other matters, as follows:

**INTRODUCTION**

1.  Plaintiff brings this action individually and on behalf of millions of other patients (collectively, the "Users") whose medical privacy was violated by Cone Health's use of tracking

1

and data collection tools by Alphabet, Inc. d/b/a Google ("Google") and Meta Platforms, Inc. d/b/a Meta ("Meta" or "Facebook").[1]

2.	Plaintiff, a Cone Health patient, alleges that Defendants installed Google and Meta Collection Tools on their public website (https://www.conehealth.com, the "Website") and their patient portal (available at https://mychart.conehealth.com, "Patient Portal") (collectively, the "Web Properties") to simultaneously collect and divulge Users' confidential health information ("Private Information" including personally identifiable information ("PII") and protected health information ("PHI")) to Google and Meta in violation of federal and state laws.

3.	Cone Health used Google Collection Tools and Meta Collection Tools to divulge the Private Information of Users of its Web Properties for marketing, re-marketing and analytics purposes despite its express promise that: "All other information that is shared in a way not addressed in this notice, including uses or disclosures for marketing purposes, or disclosures of your information in exchange for some form of payment, will be made *only after you give your written permission* or as required by law."[2]

4.	The Private Information of potentially millions of Users of Cone Health's Web Properties was improperly and unlawfully disclosed to Google and Facebook without their knowledge or consent. Cone Health did so because it knew that this sensitive information had tremendous value and that Plaintiff and Class Members would *not* consent to the collection,

---

[1] The Facebook tracking and data collection tools include the Meta Pixel, Meta SDK, Meta Conversions API, customer list uploads, social plug-ins, the Meta Graph API, server-to-server transmissions and similar collection tools (collectively, "Meta Collection Tools"). The Google tracking and collection tools include Google Analytics, Google Tag Manager, DoubleClick, social plug-ins, server-to-server transmissions and similar collection tools (collectively, "Google Collection Tools").

[2] *See* https://www.conehealth.com/patients-visitors/privacy/notice-of-privacy-practices/ (last visited May 29, 2024) (emphasis added).

disclosure and use of their Private Information if they were provided a choice or would demand significant compensation.

5.      Cone Health encouraged and/or required Plaintiff and Class Members to use its Web Properties, including its Patient Portal, to receive healthcare services, and Cone Health's Web Properties encourage and require Users to provide Private Information in order to facilitate healthcare treatment including, but not limited to, to search for a doctor, learn more about their conditions and treatments, access medical records and test results and manage appointments.

6.      At all times that Plaintiff and Class Members visited and utilized Cone Health's Website and Patient Portal to receive medical services, they had a reasonable expectation of privacy that their Private Information would remain secure and protected and only utilized for medical purposes.

7.      Further, Cone Health made express and implied promises to protect Plaintiff's and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchange with Cone Health.

8.      Simply put, Cone Health broke those promises again and again.

9.      The Facebook tracking pixel (the "Meta Pixel")—installed and configured by Cone Health—is a "piece of code" that allowed Cone Health to "measure the effectiveness of [its] advertising by understanding the actions [Users] take on [its] site."[3] It also allowed Cone Health to optimize the delivery of ads, measure cross-device conversions, create custom advertising

_____

[3]https://www.facebook.com/business/help/742478679120153?id=1205376682832142      (last visited Jun. 19, 2024).

3

groups or "audiences," learn about the use of the Web Properties and optimize advertising and marketing costs.[4]

10.     The Google Collection Tools, installed and configured by Cone Health, operate similarly to the Meta Pixel and other Meta Collection Tools.

11.     Invisible to the naked eye, pixels—which are configured by the website owners, here, Cone Health—collect and transmit information from Users' browsers to unauthorized third parties including, but not limited to, Google and Meta.[5]

12.     In particular, the Meta Pixel tracks visitors to the Web Properties and the actions they take as they interact with the website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view and the text or phrases they type into various portions of the website (such as a general search bar, chat feature or text box).[6]

13.     Cone Health purposively and intentionally installed the Google and Meta Collection Tools on its Web Properties and configured the Google and Meta Collection Tools to transmit and disclose Plaintiff's and Class Members' Private Information to Facebook.

---

[4] *Id.*

[5] The Google and Meta Collection Tools include small snippets of code placed on webpages by the website owner, for example, pixels or tags. The process of adding the Google and Meta trackers to a webpage is a multi-step process that must be undertaken by the website owner, here, Cone Health.

[6] A pixel is a piece of code that "tracks the people and type of actions they take." RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Jun. 19, 2024). Pixels are routinely used to target specific customers by utilizing the data gathered through the pixel to build profiles for the purposes of retargeting and future marketing. Upon information and belief, Cone Health utilized the data collected by the Google and Meta Collection Tools, including pixels and tags, to improve and save costs on its marketing campaign, improve its data analytics, and attract new patients.

4

14. Operating as designed, Cone Health's Google and Meta Collection Tools allowed the Private Information that Plaintiff and Class Members submitted to Cone Health to be unlawfully disclosed to Facebook.

15. For example, when a User uses Cone Health's Web Properties, the Meta Pixel and/or Google Analytics directed Plaintiff's or Class Members' browser to send a message to Facebook's/Google's servers, those messages transmitted the content of their communications to Meta/Google, including, but not limited to: (1) signing-up for the Patient Portal; (2) signing-in or -out of the Patient Portal; (3) taking actions inside the Patient Portal; (4) making, scheduling, or participating in appointments; (5) exchanging communications relating to doctors, treatments, payment information, health insurance information, prescription drugs, prescription side effects, conditions, diagnoses, prognoses, or symptoms of health conditions; (6) conduct a search on Cone Health's Web Properties and (7) other information that qualifies as PHI under federal and state laws.

16. The transmission of Plaintiff's PHI as described above occurs simultaneously from Defendant's Web Properties to both Google and Meta.

17. The information transmitted from Cone Health's Web Properties to Google and Meta includes information sufficient to identify a specific patient under federal law (such as IP address information, device identifiers, advertising identifiers that Meta associates with a patient's Facebook account and identifiers that Google associates with a patient's identity—including a unique cookie ID and/or their IP address)—and may also include a patient's demographic information, email address, phone number, computer ID address or contact information entered as emergency contacts or for advanced care planning, along with information like appointment type and date, a selected physician, button and menu selections, the content of buttons clicked and typed

5

into text boxes, and information about the substance, purport, and meaning of patient requests for information from Cone Health under federal and state health privacy laws.

18.     Among the personally identifying information that Cone Health disclosed is the User's unique and persistent Facebook ID which allows Facebook and other third parties to personally identify that User and associates the Users' Private Information with its Facebook profile. The Facebook ID is a string of numbers Facebook uses to identify and connect to a User's Facebook profile. Facebook creates a Facebook ID automatically, whether or not you choose to create a username.[7] Thus Facebook, which creates and maintains the Facebook ID directly connected to a User's Facebook account, utilizes the Facebook ID to personally identify each User whose Private Information is disclosed to it.

19.     Transmitting the Private Information allows a third party (*e.g.*, Google and/or Meta/Facebook) to know that a specific patient was seeking confidential medical care. This type of disclosure could also allow a third party to reasonably infer that a specific patient was being treated for a specific type of medical condition such as cancer, pregnancy or AIDS.

20.     Google collects the transmitted identifiable health information and uses cookies, IP addresses, and other unique identifiers to match it to Google users, allowing Cone Health to target advertisements both on and off Google. For example, Cone Health and Google can target ads to a person who has used the Website or the Patient Portal and exchanged communications about a specific condition, such as cancer.

21.     Similarly, Meta collects the transmitted identifiable health information and uses cookies, IP addresses, and other unique identifiers to match it to Facebook users allowing Cone Health to target advertisements both on and off Facebook. For example, Cone Health and Meta

---

[7] *See* https://www.facebook.com/help/211813265517027 (last visited Jun. 19, 2024).

6

can target ads to a person who has used the Website or the Patient Portal and exchanged communications about a specific condition, such as cancer.

22.     The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (1996), and state analogs prohibit healthcare providers from sharing health care information, medical records and related information with third parties except as needed for a patient's treatment, payment or with their consent.

23.     Importantly, these laws give patients a reasonable expectation of privacy in communications with healthcare providers relating to their medical conditions and treatment, because this information may not be disclosed outside the healthcare setting without notice and consent.

24.     The Office for Civil Rights ("OCR") at the United States Department of Health and Human Services ("HHS") recently re-affirmed that HIPAA and its regulations prohibit the transmittal of individually identifiable health information ("IIHI") by tracking technology like the Meta Pixel without the patient's authorization and other protections like a business associate agreement with the recipient of patient data.[8]

---

[8] *See* Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (noting that "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 in some circumstances IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services."). This guidance was recently vacated *in part* by a federal district court in the Northern District of Texas due to the court finding it in part to be the product of improper rulemaking, and it is cited for reference only until the OCR updates its guidance, should it do so in the future. *See American Hosp. Ass'n. v. Becerra*, 2024 WL 3075865 (S.D. Tex., Jun. 20, 2024). Notably, the Court's Order found only that the OCR's guidance regarding covered entities collection and disclosure to third parties of users' IP addresses while they navigated *unauthenticated public webpages* ("UPWs") was improper rulemaking. The Order in no way affects or undermines the OCR's guidance regarding covered entities disclosing unique personal identifiers, such as Google or Facebook identifiers, to third

7

25.     Reiterating the importance of and necessity for data security and privacy concerning health information, the Federal Trade Commission ("FTC") recently published a bulletin entitled *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases*, in which it noted that:

> [h]ealth information is not just about medications, procedures, and diagnoses. ***Rather, it is anything that conveys information—or enables an inference—about a consumer's health***. Indeed, [recent FTC enforcement actions involving] *Premom*, *BetterHelp*, *GoodRx* and *Flo Health* ***make clear that the fact that a consumer is using a particular health-related app or website—one related to mental health or fertility, for example—or how they interact with that app (say, turning 'pregnancy mode' on or off) may itself be health information.***[9]

26.     The FTC is unequivocal in its stance as it informs—in no uncertain terms—healthcare companies that they should ***not*** use tracking technologies to collect sensitive health information and disclose it to various platforms without informed consent:

> **Don't use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.**
>
> In today's surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. <u>***But when companies use***</u>

---

parties while patients were making appointments for particular conditions, paying medical bills or logging into (or using) a patient portal. *See id.* at 3-4, 31, n. 8 (vacating the OCR guidance with respect to the "Proscribed Combination" defined as "circumstances where an online technology connects (1) an individual's IP address with (2) a visit to a UPW addressing specific health conditions or healthcare providers" but stating that "[s]uch vacatur is not intended to, and should not be construed as, limiting the legal operability of other guidance in the germane HHS document."). Furthermore, the Federal Trade Commission's ("FTC) bulletin on the same topics remains untouched as do the FTC's enforcement actions against numerous healthcare providers for using similar (if not identical) collection tools as Cone Health.

[9]*See* Elisa Jillison, *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases,* the FTC Business Blog (July 25, 2023) (emphasis added), available at https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases (last visited Apr. 19, 2024).

> *consumers' sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.*
>
> [Recent FTC enforcement actions such as] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that *may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers' affirmative express consent for the disclosure of sensitive health information*.[10]

27. Not only did Cone Health willfully and intentionally incorporate the Google and Meta Collection Tools into its Web Properties, but it also never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications via the Web Properties with Google or Facebook.

28. As a result, Plaintiff and Class Members were unaware that their PII and/or PHI were being surreptitiously transmitted to Facebook and Google as they communicated with their healthcare providers, looked up their conditions and/or treatments, and logged into the Patient portal.[11]

---

[10] *Id.* (emphasis added) (further noting that *GoodRx* & *Premom* underscore that this conduct may also violate the Health Breach Notification Rule, which requires notification to consumers, the FTC and, in some cases, the media, of disclosures of health information without consumers' authorization.

[11] In contrast to Cone Health, several healthcare providers which have installed the Meta Pixel on their Web Properties have provided their patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. *See*, *e.g.*, *Cerebral, Inc. Notice of HIPAA Privacy Breach*, https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf (last visited Apr. 19, 2024); Annie Burky, *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies,* FIERCE HEALTHCARE (October 20, 2022), https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3 (last visited Jun. 19, 2024); *Novant Health Notifies 1.3M Patients of Unauthorized PHI Disclosure Caused By Meta Pixel* (August 17, 2022), https://healthitsecurity.com/news/novant-health-notifies-patients-of-unauthorized-phi-disclosure-caused-by-meta-

29.     The full extent of Cone Health's unlawful disclosures is not yet known, but the numbers may be staggering. According to Cone Health's Website, they employ "more than 13,000 employees, 1,800 physician partners and 1,000 volunteers" across "more than 150 locations."[12]

30.     Cone Health owed common law, contractual, statutory and regulatory duties to keep Users' communications and medical information safe, secure and confidential. Furthermore, by obtaining, collecting, using and deriving a benefit from Users' Private Information, Cone Health assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized disclosure.

31.     Cone Health, however, failed in its obligations and promises by utilizing Google and Meta Collection Tools on the Web Properties, such as Google Analytics and the Meta Pixel, knowing that such technology would transmit and share Plaintiff's and Class Members' Private Information with unauthorized third parties.

32.     Cone Health breached its obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web-based technology to ensure its Web Properties were safe and secure; (ii) failing to remove or disengage technology that was known and designed to share Users' information; (iii) failing to obtain the consent of Plaintiff and Class Members to disclose their Private Information to Google, Facebook, or others; (iv) failing to take steps to block the transmission of Plaintiff's and Class Members' Private Information through the Google and Meta Collection Tools or any other tracking technologies;  (v) failing to warn Plaintiff

---

pixel#:~:text=August%2017%2C%202022%20%2D%20North%20Carolina,protected%20health%20information%20(PHI) (last visited Jun. 19, 2024).

[12] *See* https://www.conehealth.com/about-us/ (last accessed May 29, 2024).

and Class Members; and (vi) otherwise failing to design, and monitor its Web Properties in order to maintain the confidentiality and integrity of patient Private Information.

33.     Cone Health's interception, dissemination and use of Private Information not only violates federal and state law but also harms patients by intruding upon their privacy; erodes the confidential nature of the provider-patient relationship; takes patients' property and property rights without compensation and ignores their right to control the dissemination of their health information to third parties.[13]

34.     Cone Health has also been unjustly enriched by its misconduct, obtaining unearned revenues derived from the enhanced advertising services and more cost-efficient marketing on Facebook and Google it receives in exchange for its unauthorized disclosure of patient information.

35.     Plaintiff seeks to remedy these harms individually and for millions of similarly affected persons, and therefore brings causes of action for (i) Violation of the Electronic Communications Privacy Act 18 U.S.C. § 2511(1), *et seq.*; (ii) Breach of Express Contract; (iii) Breach of Implied Duty of Good Faith and Fair Dealing; (iv) Breach of Implied Contract; (v) Negligence; (vi) Breach of Fiduciary Duty and (vii) Unjust Enrichment.

## PARTIES

36.     Plaintiff Ashika Singh is a natural person, citizen of North Carolina and a resident of Guilford County, North Carolina.

---

[13]  It is unknown without discovery whether the Private Information was further disseminated to additional third-party marketing companies (*e.g.*, Twitter, Bing, LinkedIn, HotJar, LifePerson, CrazyEgg, BlueKai, Bidtellect, Yahoo, The Trade Desk, Adobe or others) for the purposes of building or enhancing profiles and retargeting or to insurance companies to set rates, among other things.

37.     Defendant The Moses H. Cone Memorial Hospital d/b/a Cone Health is a North Carolina company with its principal place of business at 2626 Glenwood Ave. Ste 550 in Raleigh, North Carolina 27608. Defendant is "the largest and most comprehensive medical center within [the] five-county region."[14]

38.     Defendant The Moses H. Cone Memorial Hospital Operating Corporation d/b/a Cone Health is a North Carolina company and the parent company of Defendant The Moses H. Cone Memorial Hospital d/b/a Cone Health. Its principal place of business is 1200 North Elm Street in Greensboro, North Carolina 27401. Defendant is a North Carolina-wide integrated network of physician clinics, outpatient centers and hospitals. Its network consists of over 13,000 employees and 1,800 physician partners across more than 150 locations.[15] For the fiscal year ending September 2022, its revenue was over $1.6 billion, its net income was over $36 million, and its net assets were over $1.2 billion.[15]

39.     Headquartered in Greensboro, Cone Health is one of the largest health systems in the state of North Carolina. Cone Health advertises "excellent, innovative, patient-focused and comprehensive care" to the communities of Alamance, Forsyth, Guilford, Randolph, Rockingham, and surrounding counties.[16]

40.     Cone Health is a covered entity under HIPAA.

---

[14] *See* https://www.conehealth.com/locations/moses-cone-memorial-hospital/ (last accessed May 29, 2024).

[15]*See* https://projects.propublica.org/nonprofits/organizations/581588823/202312269349300781/full (last visited May 29, 2024).

[16] *See* https://www.conehealth.com/about-us/ (last visited May 29,2024)

12

## JURISDICTION & VENUE

41.     This Court has subject matter jurisdiction under 28 U.S.C. § 1331 over the claims that arise under federal law, including the Electronic Communications Privacy Act ("ECPA"), 28 U.S.C. § 2511, *et seq.*

42.     The Court has supplemental jurisdiction over Plaintiff's claims arising under state law under 28 U.S.C. § 1367.

43.     This Court also has subject matter jurisdiction under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than one hundred members in the proposed Class, and at least one member of the class is a citizen of a state different from Cone Health.

44.     This Court has personal jurisdiction over Defendants because their principal places of business are in this District and a substantial portion of the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

45.     Venue is proper under 28 U.S.C. § 1391(b)(1) and (2) because Defendants reside in this district and a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this district.

## FACTUAL BACKGROUND

**I.     CONE HEALTH SECRETLY DISCLOSED & PERMITTED THIRD PARTIES TO INTERCEPT PLAINTIFF'S & CLASS MEMBERS' PHI.**

46.     Cone Health maintains and operates the Web Properties, by and through which it encouraged and/or required patients to seek healthcare services.

47.     To obtain healthcare services through the Web Properties, Plaintiff and other Class Members were required to provide their PHI and/or PII to Cone Health.

48.     Each step of this process was tracked and logged by the Google and Meta

13

Collection Tools.

49.      On information and good faith belief, throughout the Class Period, the process for obtaining healthcare services on the Web Properties has been substantially the same in all material respects throughout the United States.

50.      Completely unbeknownst to Plaintiff and other Class Members, beginning as early as approximately October 2015 and continuing through present, Private Information that they communicated to Cone Health through the Web Properties while obtaining healthcare services was disclosed to Google.

51.      Completely unbeknownst to Plaintiff and other Class Members, from approximately September 2016 to at least July 5, 2022, Private Information that they communicated to Cone Health through the Website while obtaining healthcare services was disclosed to Meta.

**A.      *Cone Health Improperly Disclosed Plaintiff's & Class Members' Private Information to Meta.***

52.      Cone Health utilized Facebook advertisements and intentionally installed the Meta Pixel on its Web Properties.

53.      Meta's Health division is dedicated to marketing to and servicing Meta's healthcare Partners. Meta defines its Partners to include businesses that use Meta's products, including the Meta Pixel or Meta Audience Network tools to advertise, market, or support their products and services.

54.      Meta works with hundreds of Meta healthcare Partners, using Meta Collection Tools to learn about visitors to their websites and leverage that information to sell targeted

14

advertising based on patients' online behavior. Meta's healthcare Partners also use Meta's other

ad targeting tools, including tools that involve uploading patient lists to Meta.[17]

55.    Meta offers an ad targeting option called "Custom Audiences." When a patient

takes an action on a Meta healthcare Partner's website embedded with the Meta Pixel, the Meta

Pixel will be triggered to send Meta "Event" data that Meta matches to its Users. A web developer

can then create a "Custom Audience" based on Events to target ads to those patients. The Meta

Pixel can then be used to measure the effectiveness of an advertising campaign.[18]

56.    Meta also allows Meta healthcare Partners to create a Custom Audience by

uploading a patient list to Meta. As Meta describes it:[19]

A Custom Audience made from a customer list is a type of audience you can create to connect with people who have already shown an interest in your business or product. It's made of information – called "identifiers" – you've collected about your customers (such as email, phone number and address) and provided to Meta. Prior to use, Meta hashes this information.

Then, we use a process called matching to match the hashed information with Meta technologies profiles so that you can advertise to your customers on Facebook, Instagram and Meta Audience Network. The more information you can provide, the better the match rate (which means our ability to make the matches). Meta doesn't learn any new identifying information about your customers.

---

[17]    Meta Business Help Center, *About Customer List Custom Audiences* (2023), https://www.facebook.com/business/help/341425252616329?id=2469097953376494.

[18]    Meta Business Help Center, *About Customer List Custom Audiences* (2023), *https://www.facebook.com/business/help/341425252616329?id=2469097953376494*; *see also,* Meta Blueprint, Connect your data with the Meta Pixel and Conversion API (2023), https://www.facebookblueprint.com/student/activity/212738?fbclid=IwAR3HPO1d_fnzRCUAh KGYsLqNA-VcLTMr3G_hxxFr3GZC_uFUcymuZopeNVw#/page/5fc6e67d4a46d349e9dff7fa

[19]    Meta Business Help Center, *About Customer List Custom Audiences* (2023), https://www.facebook.com/business/help/341425252616329?id=2469097953376494.

15

57.     Meta provides detailed instructions for healthcare Partners to send their patients' individually identifiable information to Meta through the customer list upload. For example:

> **Prepare your customer list in advance.** To make a Custom Audience from a customer list, you provide us with information about your existing customers and we match this information with Meta profiles. The information on a customer list is known as an "identifier" (such as email, phone number, address) and we use it to help you find the audiences you want your ads to reach.
>
> Your customer list can either be a CSV or TXT file that includes these identifiers. To get the best match rates, use as many identifiers as possible while following our formatting guidelines. You can hover over the identifiers to display the formatting rules and the correct column header. For example, **first name** would appear as **fn** as a column header in your list.
>
> Alternatively, we have a file template you can download to help our system map to your identifiers more easily. (You can upload from Mailchimp as well.)

58.     Meta healthcare Partners can then use the Custom Audiences derived from their patient list with the Meta Pixel and Pixel Events for Meta marketing campaigns and to measure the success of those campaigns.

59.     Without discovery, Plaintiff does not yet know whether Cone Health uploaded patient lists to Meta. However, Plaintiff does know that when they and Class Members sought and used Cone Health's Web Properties, their Private Information was intercepted concurrently in real time and then disseminated to Facebook and potentially to other third parties, via the Meta Pixel and other Meta Collection Tools that Cone Health secretly installed on the Web Properties.

60.     Plaintiff and Class Members did not intend or have any reason to suspect their Private Information would be shared with Facebook or that Cone Health was tracking their every movement and disclosing same to Facebook when they entered highly sensitive information on the Web Properties.

61.     Cone Health did not disclose to or warn Plaintiff or Class Members that Cone Health used Plaintiff's and Class Members' Web Properties submissions for Facebook's marketing purposes.

16

62.    Plaintiff and Class Members never consented, agreed, authorized or otherwise permitted Cone Health to disclose their Private Information to Meta.

63.    On information and good faith belief, Cone Health's unauthorized disclosure is not just limited to activity on the public Website, but the disclosure also involved information contained within the highly sensitive and private Patient Portal, which requires patients to enter a specific login.

64.    Cone Health disclosed to Meta the following non-public private information:

a.  when a patient sets up or schedules an appointment;

b.  information that a patient types into or chooses on an appointment form;

c.  when a patient clicks a button to call the provider from a mobile device directly from the Website;

d.  descriptive URLs that describe the categories of the Website, categories that describe the current section of the Website, and the referrer URL that caused navigation to the current page;

e.  the communications a patient exchanges through Cone Health's Web Properties by clicking and viewing webpages, including communications about providers and specialists, conditions, and treatments, along with the timing of those communications, including—upon information and belief—whether they are made while a patient is still logged in to the Patient Portal or around the same time that the patient has scheduled an appointment, called the medical provider, or logged into the Patient Portal; and

f.  the same or substantially similar communications that patients exchange with health insurance companies, pharmacies, and prescription drug companies.

65.    Cone Health deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented technology (i.e. Meta Pixels) that surreptitiously tracked, recorded and disclosed Plaintiff's and other Users' confidential communications and Private Information; (2) disclosed

17

patients' protected information to Meta—an unauthorized third party and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

**B.** ***Meta's Collection Tools Redirect Patients' Data from Cone Health's Web Properties to Facebook to Use for Ad Targeting.***

66. Facebook operates the world's largest social media company and generated nearly $117 billion in revenue in 2022, roughly 97% of which came from selling targeted advertising. [20]

67. As a core part of its business, Facebook maintains profiles on users that include the user's real names, locations, email addresses, friends, likes and communications that Facebook associates with personal identifiers, including IP addresses, cookies, device identifiers and advertising ID identifiers.

68. Facebook also tracks non-Facebook users through its widespread internet marketing products and various tracking codes, such as the Meta Pixel, tracking scripts and cookies.

69. Facebook then sells advertising space by highlighting its ability to target users.[21] Facebook can target users so effectively because it surveils user activity both on and off its site.[22]

---

[20] FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2022 RESULTS, https://investor.fb.com/investor-news/press-release-details/2023/Meta-Reports-Fourth-Quarter-and-Full-Year-2022-Results/default.aspx (last visited Jun. 12, 2024).

[21] WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706 (last visited Jun. 12, 2024).

[22] ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Jan. 12, 2024).

18

This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[23]

70.     Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[24]

71.     Indeed, Facebook utilizes the precise type of information disclosed by Cone Health to identify, target, and market products and services to individuals.

72.     Advertisers can also build "Custom Audiences."[25] Custom Audiences enable advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[26]

73.     With Custom Audiences, advertisers can target existing customers directly, and they can also build "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[27]

---

[23] AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited Jun. 12, 2024).

[24] EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences (last visited Jun. 12, 2024).

[25] ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494 (last visited Jun. 12, 2024).

[26] AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited Jun. 12, 2024).

[27]                    ABOUT                    LOOKALIKE                    AUDIENCES, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last visited Jun. 12, 2024).

74.     Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences *only if they first supply Facebook with the underlying data*. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook's "Business Tools."[28]

75.     As Facebook puts it, the Business Tools "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[29]

76.     Put more succinctly, Facebook's Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

77.     The Business Tools are automatically configured to capture certain data, like when a User visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[30]

---

[28]     CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; Facebook, Create a Website Custom Audience https://www.facebook.com/business/help/1474662202748341?id=2469097953376494 (last visited Jun. 12, 2024).

[29] THE FACEBOOK BUSINESS TOOLS, https://www.facebook.com/help/331509497253087 (last visited Jun. 12, 2024).

[30]     *See* FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Jun. 19, 2024).

20

78.     Facebook's Business Tools can also track other events. Facebook offers a menu of "standard events" from which advertisers can choose, including what content a visitor views or purchases.[31] Advertisers can even create their own tracking parameters by building a "custom event." [32]

79.     One such Business Tool is the Meta Pixel. Facebook offers this code to advertisers, like Cone Health, to integrate into their website. As the name implies, the Meta Pixel "tracks the people and type of actions they take."[33]

80.     Meta pushes advertisers to install the Meta Pixel. Meta tells advertisers the Pixel "can help you better understand the effectiveness of your advertising and the actions people take on your site, like visiting a page or adding an item to their cart."[34]

81.     Meta tells advertisers that the Meta Pixel will improve their Facebook advertising, including by allowing them to:

> a. "measure cross-device conversions" and "understand how your cross-device ads help influence conversion";
>
> b. "optimize the delivery of your ads" and "[e]nsure your ads reach the people most likely to take action" and

---

[31]     SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited Jun. 19, 2024).

[32]     ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/. (last visited Jun. 19, 2024).

[33] RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Jun. 11, 2024).

[34] Meta, Meta Pixel (2023), https://www.facebook.com/business/tools/meta-pixel.

c. "create Custom Audiences from website visitors" and create "[d]ynamic ads [to] help you automatically show website visitors the products they viewed on your website—or related ones."[35]

82. Meta explains that the Meta Pixel "log[s] when someone takes an action on your website" such as "adding an item to their shopping cart or making a purchase," and the user's subsequent action:



Once you've set up the Meta Pixel, the Pixel will log when someone takes an action on your website. Examples of actions include adding an item to their shopping cart or making a purchase. The Meta Pixel receives these actions, or events, which you can view on your Meta Pixel page in Events Manager. From there, you'll be able to see the actions that your customers take. You'll also have options to reach those customers again through future Facebook ads.

83. The Meta Pixel is customizable, meaning web developers can choose the actions the Pixel will track and measure.

84. Meta advises web developers to place the Meta Pixel early in the source code for any given webpage or website to ensure that visitors will be tracked before they leave the webpage or website:

---

[35] *Id.*

22

## Installing The Pixel

To install the pixel, we highly recommend that you add its base code between the opening and closing `<head>` tags on every page where you will be tracking website visitor actions. Most developers add it to their website's persistent header, so it can be used on all pages.

Placing the code within your `<head>` tags reduces the chances of browsers or third-party code blocking the pixel's execution. It also executes the code sooner, increasing the chance that your visitors are tracked before they leave your page.

85. Meta also provides advertisers with step-by-step instructions for setting up and installing the Meta Pixel on their website, so that companies can add the Meta Pixel to their website without a developer.[36]

86. If a healthcare provider, such as Cone Health, installs the Meta Pixel code as Meta recommends, patients' actions on the provider's website are contemporaneously redirected to Meta. When a patient clicks a button to register for, or logs into or out of, a "secure" patient portal, Meta's source code commands the patient's computing device to send the content of the patient's communication to Meta while the patient is communicating with her healthcare provider—traveling directly from the user's browser to Facebook's server.

87. In other words, by design, Meta receives the content of a patient's portal log in communication immediately when the patient clicks the log-in button—even before the healthcare provider receives it.

88. This contemporaneous and secret transmission contains the original GET request sent to the host website, along with additional data that the Meta Pixel is configured to collect. This transmission is initiated by the Facebook code installed by Cone Health and concurrent with the Users' communications with the host website. Two sets of code are thus automatically run as

---

[36] Meta, *Meta Pixel* (2023), https://www.facebook.com/business/tools/meta-pixel.

23

part of the browser's attempt to load and read the Cone Health's Web Properties— Cone Health's

own code, and the Facebook code Cone Health embedded.

89.     Thus, the Meta "pixel allows Facebook to be a silent third-party watching whatever

you're doing."[37]

90.     Cone Health, through its installation and use of the Meta Pixel, disclosed to Meta

the content of patient communications while its patients were exchanging communications with

Cone Health's Web Properties.

91.     Cone Health's use of the Meta Pixel to send Facebook the names and/or specialty

of patients' doctors or their appointment-related details would have permitted Cone Health to

specifically target its existing patients with Facebook ads *based on their health conditions*, as well

as create Lookalike Audiences for the same purpose. This could only be accomplished by Cone

Health disclosing to Meta the content of those patients' communications on Cone Health's Web

Properties, providing Facebook with a list of Cone Health's patients, or otherwise disclosing the

identity of Cone Health's patients to Meta through the Meta Collection Tools.

### C.     *Cone Health Improperly Disclosed Plaintiff's & Class Members' Private Information to Google.*

92.     Cone Health utilized Google advertisements and intentionally installed the Google

Collection Tools on its Web Properties, including but not limited to Google Analytics, Google Tag

Manager, and DoubleClick Ad trackers.

---

[37] Jefferson Graham, *Facebook spies on us but not by recording our calls. Here's how the social network knows everything*, USA Today (March 4, 2020 4:52 am), https://www.usatoday.com/story/tech/2020/03/04/facebook-not-recording-our-calls-but-has-other-ways-snoop/4795519002/#.

93.     Cone Health installed a Google Analytics tracker, Google Tag Manager, and DoubleClick Ad trackers beginning in at least October 2015 and continued to disclose its patient's data to Google through at least May 21, 2024.

94.     Google offers an ad targeting option called "Custom Audiences." When a patient takes an action on a Google healthcare Partner's website embedded with Google tracking code, the tracking code will be triggered to send Google "Event" data that Google matches to its Users. A web developer can then create a "Custom Audience" based on Events to target ads to those patients. The Google tracking code can then be used to measure the effectiveness of an advertising campaign.[38]

95.     When Plaintiff and Class Members sought and used Cone Health's Web Properties, their Private Information was intercepted concurrently in real time and then disseminated to Google and potentially to other third parties, via the Google tracking code and other Google Collection Tools that Cone Health secretly installed on the Web Properties.

96.     Plaintiff and Class Members did not intend or have any reason to suspect their Private Information would be shared with Google or that Cone Health was tracking their every movement and disclosing same to Google when they entered highly sensitive information on Cone Health's Web Properties.

97.     Cone Health did not disclose to or warn Plaintiff or Class Members that Cone Health used Plaintiff's and Class Members' Web Properties submissions for Google's marketing purposes.

---

[38]     Google Ads API, *Custom Audiences*, https://developers.google.com/google-ads/api/docs/remarketing/audience-segments/custom-audiences#how_custom_audiences_work (last visited May 29, 2024)

25

98.     Plaintiff and Class Members never consented, agreed, authorized or otherwise permitted Cone Health to disclose their Private Information to Google.

99.     Cone Health's unauthorized disclosure is not just limited to activity on the public Website, but the disclosure also involved information contained within the highly sensitive and private Patient Portal, which requires patients to enter a specific login.

100.    Cone Health disclosed to Google the following non-public private information:

   a. Details about users' activities on Cone Health's Web Properties;

   b. The exact date, time, and location from which a user first entered Cone Health's Web Properties at https://www.conehealth.com/;

   c. Information that a user is actively on Cone Health's homepage, and each subsequent click on Cone Health's Web Properties is transmitted to Google;

   d. Keyword searches, Location, and Physician Searches;

   e. Appointment scheduling activities;

   f. when a patient clicks to sign up for the Patient Portal;

   g. when a patient clicks to log in to the Patient Portal;

   h. when a patient views Cone Health's services related to specific conditions; and

   i. other activities that reveal users' patient status.

101.    Further, the data from 'events' captured by Defendant's Google Analytics tracker shows that Cone Health has not enabled IP Masking and transmits user IP addresses to Google alongside their PHI.

102.    Cone Health deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented technology (*i.e.,* Google Collection Tools) that surreptitiously tracked, recorded and disclosed Plaintiff's and other Users' confidential communications and Private Information;

26

(2) disclosed patients' protected information to Google—an unauthorized third party and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

### D. Google's Collection Tools Redirect Patients' Data from Cone Health's Web Properties to Google to Use for Ad Targeting.

103. Google operates the world's largest internet search engine company and generated roughly $307 billion in revenue in 2023, roughly 76% of which came from selling advertising. [39]

104. As a core part of its business, Google maintains profiles on users of its products (e.g, Gmail, Google Search, Chrome browser, YouTube or Google devices) that include the user's real names, locations, email addresses, friends, internet activity, and communications that Google associates with personal identifiers, including IP addresses, cookies, device identifiers and advertising ID identifiers.

105. Google also tracks people regardless of whether they use Google products through its widespread internet marketing products and ubiquitous trackers.

106. Google then sells advertising space by highlighting its ability to target users. [40] Google can target users so effectively because it surveils user activity both on and off Google sites and apps. This allows Google to make inferences about users beyond what they explicitly disclose,

---

[39] ALPHABET, INC REPORTS FOURTH QUARTER AND FULL YEAR 2023 RESULTS, https://abc.xyz/assets/95/eb/9cef90184e09bac553796896c633/2023q4-alphabet-earnings-release.pdf (last visited May 29, 2024).

[40] BENEFITS OF ONLINE ADVERTISING AND GOOGLE ADS, https://support.google.com/google-ads/answer/6123875?hl=en#:~:text=Control%20your%20costs,per%20day%2C%20and%20per%20ad. (last visited May 29, 2024).

determining audiences by "[users'] activity using Google products and third-party websites, or estimated based on content certain groups of people are likely to be interested in."[41]

107. Google compiles this information into a generalized dataset called "Audience Segments," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[42]

108. Indeed, Google utilizes the precise type of information disclosed by Cone Health to identify, target, and market products and services to individuals.

109. Advertisers can also select "Custom Audiences."[43] Custom Audiences enable advertisers to reach "your ideal audience by entering relevant keywords, URLs, and apps."[44]

110. With Custom Audiences, advertisers can target existing customers directly, and they can also build Audiences similar to their existing customers.

111. As Google puts it, the Google Analytics "Google Analytics is a platform that collects data from your websites and apps to create reports that provide insights into your business."[45]

---

[41] ABOUT AUDIENCE SEGMENTS,
https://support.google.com/google-ads/answer/2497941?sjid=6716156162402223675-NA (last visited May 29, 2024).

[42] Id.

[43] CUSTOM AUDIENCES,
https://developers.google.com/google-ads/api/docs/remarketing/audience-segments/custom-audiences#how_custom_audiences_work (last visited June 12, 2024).

[44] Id.

[45] HOW GOOGLE ANALYTICS WORKS,
https://support.google.com/analytics/answer/12159447?hl=en (last visited May 29, 2024).

28

112.    Put more succinctly, Google Analytics, Google Tag Manager and DoubleClick are bits of code that advertisers can integrate into their websites, mobile applications, and servers, thereby enabling Google to intercept and collect user activity on those platforms.

113.    Google Analytics is automatically configured to capture certain data, like when a User visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[46]

114.    Google Analytics can also track other events. Google offers a menu of "standard events" from which advertisers can choose, including what content a visitor views or purchases.[47] Advertisers can even create their own tracking parameters by building a "custom event." [48]

115.    Google offers this code to advertisers, like Cone Health, to integrate into their website. Google Analytics tracks "how many users perform the action and evaluate marketing performance across all channels that lead users to perform the action… A key event is an event that measures an action that's particularly important to the success of your business. When someone triggers the event by performing the action, the key event is recorded in Google Analytics and surfaced in your Google Analytics reports."[49]

---

[46]      GOOGLE      ANALYTICS      –      THE      FINER      POINTS
https://marketingplatform.google.com/about/analytics/features/ (last visited May 29, 2024).

[47] *Id.*

[48] *Id.*

[49]GOOGLE      ANALYTICS      HELP      -      ABOUT      KEY      EVENTS,
https://support.google.com/analytics/answer/9267568?hl=en (last visited May 29, 2024).

29

116.    Google pushes advertisers to install Google Analytics. Google says Analytics "can track what online behavior led to purchases and use that data to make informed decisions about how to reach new and existing customers."[50]

117.    Google tells advertisers that Google Analytics will improve their Google advertising through the following features:

    a.  "Collects both website and app data to better understand the customer journey;

    b.  Uses event-based data instead of session-based;

    c.  Includes privacy controls such as cookieless measurement, and behavioral and key event modeling;

    d.  Predictive capabilities offer guidance without complex models;

    e.  Direct integrations to media platforms help drive actions on your website or app."[51]

118.    Google explains that Google Analytics logs consumer actions, such as clicking a button, called "events":[52]

---

[50]    GOOGLE ANALYTICS HELP – THE VALUE OF DIGITAL ANALYTICS, https://support.google.com/analytics/answer/12159453?hl=en&sjid=8517741530658858223-NA&visit_id=638526037873608158-2523537901&rd=2&ref_topic=14089939 (last visited May 29, 2024).

[51]    GOOGLE ANALYTICS HELP – SET UP ANALYTICS FOR A WEBSITE AND/OR APP https://support.google.com/analytics/answer/9304153?sjid=8517741530658858223-NA (last visited May 29, 2024).

[52] *Id.*

30

## How it works

Let's say someone clicks a link on your tagged website that takes them to an external website. The following illustrates what happens when the user clicks the link:



|  |  |  |  |
| :---: | :---: | :---: | :---: |
| **1** | **2** | **3** | **4** |
| The user visits your website and clicks a link to an external website | Analytics receives the click event and surfaces the event and parameters in the Realtime report | Analytics fully processes the event | Analytics surfaces the data in dimensions and metrics used in reports, audiences, etc. |

119.    According to Google, "An event allows you to measure a specific interaction or occurrence on your website or app. For example, you can use an event to measure when someone loads a page, clicks a link, or completes a purchase, or to measure system behavior, such as when an app crashes or an impression is served."[53]

120.    The Google Analytics tracker  is customizable. Meaning, web developers can choose the events Google Analytics  will track and measure.

---

[53] ABOUT EVENTS,
https://support.google.com/analytics/answer/9322688?hl=en#zippy=%2Crealtime-report%2Cdebugview-report (last visited May 29, 2024).

121.     Google advises web developers to place Google tracking code early in the source

code for any given webpage or website to ensure that visitors will be tracked before they leave the

webpage or website:[54]

## Set up data collection for websites

To begin seeing data in your new Google Analytics 4 property, you'll need to do one of the following:

Add the tag to a website builder or CMS-hosted website (e.g., HubSpot, Shopify, etc.)     ⌄

Add the Google tag directly to your web pages     ⌃

> You need access to the HTML for your web pages. Ask your web developer to perform these steps if you're unable to complete the steps yourself.
>
> 1. Sign in to your Google Analytics account ⧉.
> 2. Click **Admin** ⧉.
> 3. At the top of the *Property* column, select your property.
> 4. In the *Property* column, click **Data streams > Web**.
> 5. Click the data stream for your website.
> 6. Under *Google tag*, click **View tag instructions**.
> 7. On the *Installation instructions* page, select **Install manually**:
>    - On the screen, you'll see the JavaScript snippet for your account's Google tag. Your Google tag is the entire section of code that appears, beginning with:
>
>      ```
>      <!-- Google tag (gtag.js) -->
>      ```
>
>      and ending with
>
>      ```
>      </script>
>      ```
>
> Paste your Google tag immediately after the `<head>` on each page of your website.
>
> Data collection may take up to 30 minutes to begin. You can then use the Realtime report ⧉ to verify that you're receiving data.

---

32

122.     Google also provides advertisers with step-by-step instructions for setting up and installing Google tracking code on their website, so that companies can add Google tracking code to their website without a developer.[55]

123.     If a healthcare provider, such as Cone Health, installs Google Analytics code as Google recommends, patients' actions on the provider's website are contemporaneously redirected to Google. When a patient clicks a button to register for, or logs into or out of, a "secure" patient portal, Google's source code commands the patient's computing device to send the content of the patient's communication to Google while the patient is communicating with her healthcare provider—traveling directly from the user's browser to Google's server.

124.     In other words, by design, Google receives the content of a patient's portal log in communication immediately when the patient clicks the log-in button—even before the healthcare provider receives it.

125.     This contemporaneous, and secret transmission contains the original GET request sent to the host website, along with additional data that Google Analytics is configured to collect. This transmission is initiated by the Google code installed by Cone Health and concurrent with the Users' communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Cone Health's Web Properties— Cone Health's own code, and the Google code Cone Health embedded.

126.     Cone Health, through its installation and use of Google Analytics, disclosed to Google the content of patient communications while its patients were exchanging communications with Cone Health's Web Properties.

---

[55] *Id.*

33

127.     Cone Health's use of Google Analytics to send Google the names of patients' doctors would have permitted Cone Health to specifically target its existing patients with Google ads *based on their health conditions*, as well as create Audiences for the same purpose. This could only be accomplished by Cone Health disclosing to Google the content of those patients' communications on Cone Health's Web Properties, providing Google with a list of Cone Health's patients, or otherwise disclosing the identity of Cone Health's patients to Google through Google Analytics.

> **E.     *Cone Health's Use of Source Code, Google Analytics and the Meta Pixel & Interception of HTTP Requests.***

128.     Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the Internet. Each "client device" (such as a computer, tablet or smartphone) accesses web content through a web browser (e.g., Google's Chrome, Mozilla's Firefox, Apple's Safari and Microsoft's Edge).

129.     Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' client devices via web browsers.

130.     Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.

- **Cookies**: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host

34

server. Some cookies are "third-party cookies" which means they can store and communicate data when visiting one website to an entirely different website.

- **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.[56]

131.    A patient's HTTP Request essentially asks the Website to retrieve certain information (such as the name of a doctor with whom a patient makes an appointment), and the HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate the Web Properties).

132.    Every website is comprised of Markup and "Source Code." Source Code is a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

133.    Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. The Google and Meta Collection Tools and other tracking technologies Cone Health uses constitute source code that does just that. These tracking technologies thus act much like a traditional wiretap.

134.    Cone Health encourages customers to use its Web Properties to obtain healthcare services, such as making appointments with doctors and other providers and take other actions related to their personal health care. When interacting with Cone Health's Web Properties like

---

[56] One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

35

this, Plaintiff and Class Members convey highly private and sensitive information to Cone Health.

135. When patients visit Cone Health's Web Properties via an HTTP Request to Cone Health's server, that server sends an HTTP Response including the Markup that displays the webpage visible to the user and Source Code, including Cone Health's Google and Meta Collection Tools.

136. Thus, Cone Health is in essence handing patients a tapped device, and once the webpage is loaded into the patient's browser, the software-based wiretap is quietly waiting for private communications on the Web Properties to trigger the tap, which intercepts those communications intended only for Cone Health and transmits those communications to third parties, including Google and Meta.

137. Cone Health intentionally configured the Google and Meta Collection Tools installed on the Web Properties to capture both the "characteristics" of individual patients' communications with the Cone Health's Web Properties (e.g., their IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers) and the "content" of these communications (i.e., the buttons, links, pages, and tabs they click and view, as well as search terms entered into free text boxes and descriptive URLs showing the information being exchanged).

   F.   *Google and Meta Use Identifiers to Match the Health Information They Collect with Google and Facebook Users.*

138. Meta uses cookies to identify patients, including cookies named c_user, datr, fr, and _fbp.

139. The c_user cookie identifies Facebook users. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user account has one—and

36

only one—unique c_user cookie. Meta uses the c_user cookie to record user activities and communications.

140.     An unskilled computer user can obtain the c_user cookie value for any Facebook user by (1) going to the user's Facebook page, (2) right-clicking with their mouse, (3) selecting "View page source," (4) executing a control-f function for "UserID," and (5) copying the number value that appears after "UserID" in the page source code of the Facebook user's page.

141.     Following these directions makes it possible to discover that the Facebook UserID assigned to Mark Zuckerberg is 4. By typing www.facebook.com/4 into a browser and hitting enter, a browser directs to Mr. Zuckerberg's page at www.facebook.com/zuck.

142.     A user's Facebook ID is therefore linked to their Facebook profile, which contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile. To find the Facebook account associated with a c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

143.     The Meta datr cookie identifies the web browser the patient is using. It is an identifier unique to each patient's specific web browser, so it is another way Meta can identify Facebook users.

144.     Meta keeps a record of every datr cookie identifier associated with each of its users, and a Facebook user can obtain a redacted list of all datr cookies associated with his or her Facebook account from Meta by using the Facebook "Download Your Information" tool.

37

145.    The Meta fr cookie is an encrypted combination of the c_user and datr cookies.[57]

146.    The c_user, datr and fr cookies are traditional third-party cookies, meaning they are cookies associated with a party other than the entity with which a person is communicating at the time. In the case of Cone Health, they are third-party cookies because Meta is a third party to the communication between a patient and their healthcare provider.

147.    The Meta _fbp cookie is a Facebook identifier that is set by Facebook source code and associated with the healthcare provider using the Meta Pixel.

148.    The _fbp cookie is a third-party cookie in that it is also a cookie associated with Meta that is used by Meta to associate information about a person and their communications with non-Meta entities while the person is on a non-Meta website or application.

149.    Meta disguises the _fbp cookie as a first-party cookie even though it is Meta's cookie on non-Meta websites.

150.    By disguising the _fbp cookie as a first-party cookie for a healthcare provider rather than a third-party cookie associated with Facebook, Meta ensures that the _fbp cookie is placed on the computing device of patients who seek to access the patient portal.

151.    Healthcare providers with a patient portal require patients to enable first-party cookies to gain access to their patient records through the portal.

152.    The purpose of these portal-associated first-party cookies is security. The _fbp cookie is then used as a unique identifier for that patient by Meta. If a patient takes an action to delete or clear third-party cookies from their device, the _fbp cookie is not impacted—even though it is a Meta cookie—again, because Meta has disguised it as a first-party cookie. Meta

---

[57] *See* Gunes Acar, *et al.*, *Facebook Tracking Through Social Plug-ins: Technical Report Prepared for the Belgian Privacy Commission* (Mar. 27, 2015), https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf.

also uses IP address and user-agent information to match the health information it collects from Meta healthcare Partners with Facebook users.

153.    Google uses similar tools to track users of websites with Google tracking code installed, such as Google Analytics.

154.    Universal Analytics is an older version of Google Analytics that was installed on the Web Properties by default prior to October 2020 that collected and stored IP addresses of users of the Web Properties in addition to other unique patient identifiers, including the cid parameter cookie.[58]

155.    Cone Health began installing a Universal Analytics tracker with ID UA-35381524-1 (and other Google Collection Tools) as early as September 2016.

156.    Universal Analytics tracks, among other types of data, "events" which include instances when a patient downloads a document, engages with a webpage by putting in their login information, or navigates to a certain part of the webpage and clicks a button.

157.    For these Universal Analytics events, Cone Health needed to opt-in to IP Masking to stop Google from collecting users' IP addresses. Plaintiff's investigation to-date indicates that, based on the absence of an "aip=1" parameter in Defendant's Universal Analytics events, Cone Health did not enable IP Masking. Consequently, Google collected and stored IP addresses from Cone Health users.

158.    Google DoubleClick events are also linked to Universal Analytics events. Each DoubleClick event includes the Universal Analytics event's 'tid'. The 'tid' is the tag ID of the

---

[58]    https://www.fullmedia.com/based-on-the-new-hhs-guidance-is-google-analytics-hipaa-compliant (last accessed June 17, 2024).

Universal Analytics tracking code used by Cone Health, and it's how Google identifies Cone Health's Google Analytics account.

159.    Each DoubleClick event also includes the 'cid' parameter. The 'cid' parameter is a first-party cookie that helps Google identify Cone Health's users.  Consequently, Google can connect DoubleClick and Universal Analytics events with individual users of Cone Health's Web Properties.

160.    A first-party cookie, unique to Cone Health's Website, differs from third-party cookies in that it will not be identical when a user visits another website.

161.    Accordingly, Cone Health's Web Properties through the Google and Meta Collection Tools and other tracking technologies routinely provide Facebook and Google with Cone Health's patients' Facebook IDs or cid parameter cookies, IP addresses, and/or device IDs and the other information they input into the Web Properties, including not only their medical searches, treatment requests, and the webpages they view. This is precisely the type of identifying information that HIPAA requires healthcare providers to anonymize to protect the privacy of patients.[59] Plaintiff's and Class Members' identities can be easily determined based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

162.    After intercepting and collecting this information, Facebook processes it, analyzes it and assimilates it into datasets like Core Audiences and Custom Audiences. If the website visitor

---

[59] *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 (last visited Jun. 19, 2024).

is also a Facebook user, the information collected via the Meta Pixel is associated with the user's

Facebook ID that identifies their name and Facebook profile, i.e., their real-world identity.

163.    While the Meta Pixel tool "hashes" personal data—obscuring it through a form of

cryptography before sending the data to Facebook—that hashing does not prevent Facebook from

reading, understanding, and using the data.[60]

164.    In fact, Facebook explicitly uses the hashed information it gathers to link Pixel-

transmitted data to Facebook profiles.[61] Indeed, there would be no value in targeting Facebook

users with Cone Health's ads if Facebook couldn't read the hashed data it received from Cone

Health to know *who* to target.

165.    As Facebook explains, "[a]utomatic advanced matching will tell your pixel to look

for recognizable form fields and other sources on your website that contain information such as

first name, last name and email address. The Meta Pixel receives that information along with the

event, or action, that took place. This information gets hashed in the visitor's browser. ***We can***

***then use the hashed information to more accurately determine which people took action in***

***response to your ad***."[62]

166.    Similarly, Facebook tells businesses: "When you upload your customer list in Ads

Manager to create a Custom Audience, the information in your list is hashed before it's sent to

Facebook. ***Facebook uses this hashed information and compares it to our own hashed***

---

[60]*See*        https://www.facebook.com/business/help/112061095610075?id=2469097953376494;
https://www.facebook.com/business/help/61177468565668?id=12053%2076682832142

[61]    *See*    https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-
information-from-hospital-websites.

[62] https://www.facebook.com/business/help/61177468565668?id=12053%2076682832142.

41

*information. Then, we help build your audience by finding the Facebook profiles that match and create a Custom Audience for you from those matches.*"[63]

167.    In other words, Facebook uses its own secret language to encode and then read and match individuals' information.

168.    Facebook claims that after hashing individuals' Private Information (including their personal identifiers and PHI shared by Defendant) and matching it to Facebook profiles to create Custom Audiences, Facebook deletes the hashed data.

169.    Even assuming this is true, by that point, the damage is done—Facebook has read, understood, analyzed, and expressly taken action to match the shared PHI with specific individuals, with the express purpose of targeting those individuals with ads based on the data (PHI) that was shared and used to create Cone Health's Custom Audiences—all at Cone Health's request.

170.    Google uses a similar process to identify specific users and match their profiles with data collected by Google tracking code, such as Google Analytics, including specific actions taken by patients on websites in which Google tracking code is installed.

171.    This disclosed PHI and PII allows Facebook and Google to know that a specific patient is seeking confidential medical care and the type of medical care being sought, and in addition to permitting Cone Health to target those persons with Cone Health's ads, Facebook and Google also then sell that information to marketers who will online target Plaintiff and Class Members.

---

[63] https://www.facebook.com/business/help/112061095610075?id=2469097753376494.

**G.** *Evidence That Cone Health Installed the Meta Pixel on its Web Properties and Used the Meta Pixel to Transmit Private Information to Meta.*

172. Archives of Cone Health's Web Properties shows the installation of two Meta Pixels, ID 784395891701964 ("Meta Pixel 1") and ID 784395891701964 ("Meta Pixel 2").

173. Cone Health installed Meta Pixel 1 as early as September 25, 2016:
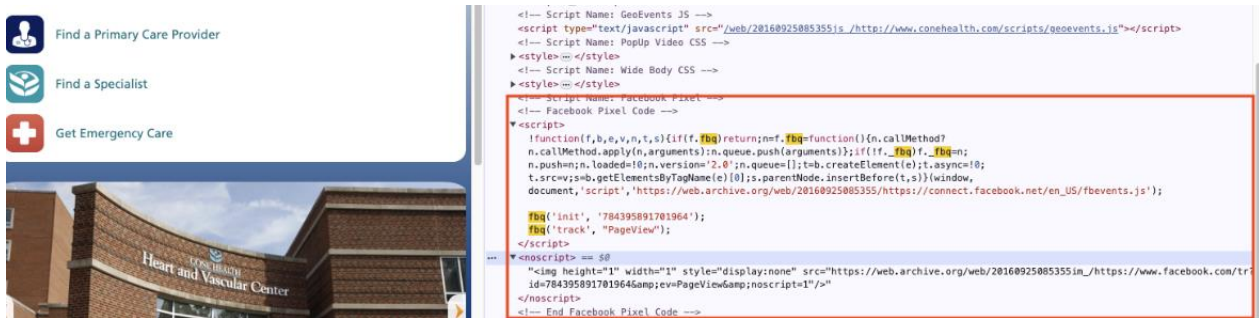


174. Cone Health installed Meta Pixel 2 as early as July 5, 2022:

ty\": \"Greensboro\"}\n\t\t\t}\n\t\t\t\t\n\n
eIframeMode":false,"vtp_enableEditJsMacroBeha
ion(b,e,f,g,a,c,d){b.fbq||(a=b.fbq=function()
Element(f),c.async=!0,c.src=g,d=e.getElements
events.js\"); fbq(\"init\",\"784395891701964\"
ght=\"1\" width=\"1\" style=\"display:none\"

175.    The Meta Pixel's configuration files demonstrate the actions that Cone Health took using the Meta Pixel that it installed and the custom events that it set up to transmit patients' Private Information to Meta.

176.    Using the Pixel installed on its Web Properties, Cone Health transmitted PageView and Microdata events about Users' activities. Upon a User's arrival on Cone Health's homepage, Cone Health immediately sent a pair of PageView and Microdata events to Facebook revealing that the user was on the page, https://www.conehealth.com. As Users navigated beyond the homepage, Cone Health continued to disclose user data including Users': (i) physician search activities; (ii) keyword search activities; (iii) appointment activities; (iv) Users' unique identifiers

44

including their Facebook ID, names, or email addresses, and (v) Patient Portal and bill payment activities.
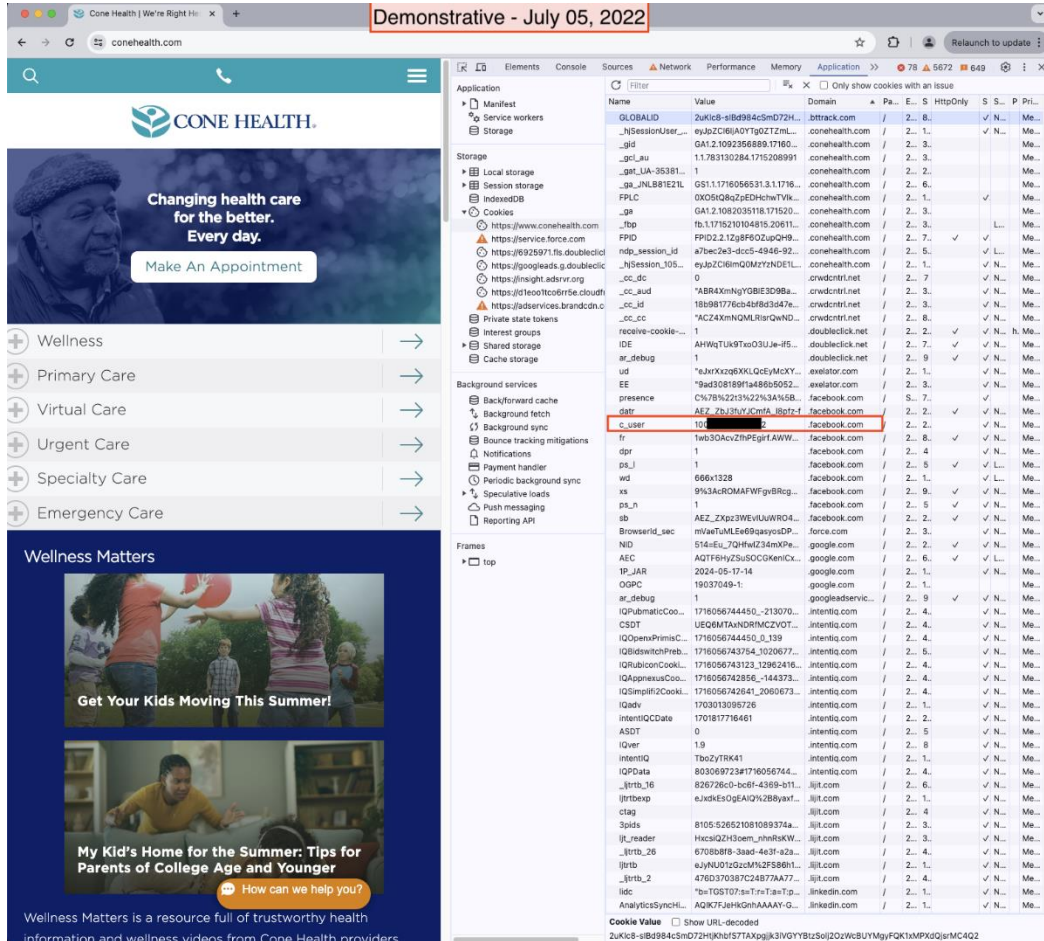


177.    In each of the transmitted Meta Pixel events, Cone Health included the "c_user" cookie, which Facebook uses to identify Users.

178. Therefore, Facebook could connect the cookie data that Cone Health transmitted with specified Users.

179. When a User searches Cone Health's Web Properties to find doctors, Cone Health sends a SubscribedButtonClick event informing Facebook that the User clicked to "Search" at https://www.conehealth.com/. Cone Health then sent a further set of PageView and Microdata events when the User loaded the page.

180. From the "Search Results" page, the User may search for a doctor by adding parameters such as providers and locations. Cone Health also sent Facebook such user parameters. As an example, when a selects conditions and searches for "cancer", Cone Health sent PageView and Microdata events which reveal that the user searched for "cancer".

181. Cone Health then discloses the User's activities as they interact with their search results. For instance, the User could click to view a physician's page, call a physician or book an appointment. As the User clicked for each action, Cone Health sent a SubscribedButtonClick event revealing the User's action and the context of the User's search for providers with a specialty of lung cancer in Greensboro, North Carolina.

46

182.    Specifically, when the User clicked to view a physician's profile, the SubscribedButtonClick event Cone Health sent reveals that the user clicked on a button labeled "Need Care? Make an Appointment," on a page for lung cancer:

**H.** **Evidence That Cone Health Installed Google Collection Tools on its Web Properties and Used Google Analytics to Transmit Private Information to Google.**

183. A review of Cone Health's Web Properties shows the installation of the Google Analytics Tracker with ID UA- 35381524-1 ("UA1"), a Google Tag Manager Container with ID GTM-NM29WS ("GTM1"), and DoubleClick Ads at that same time:
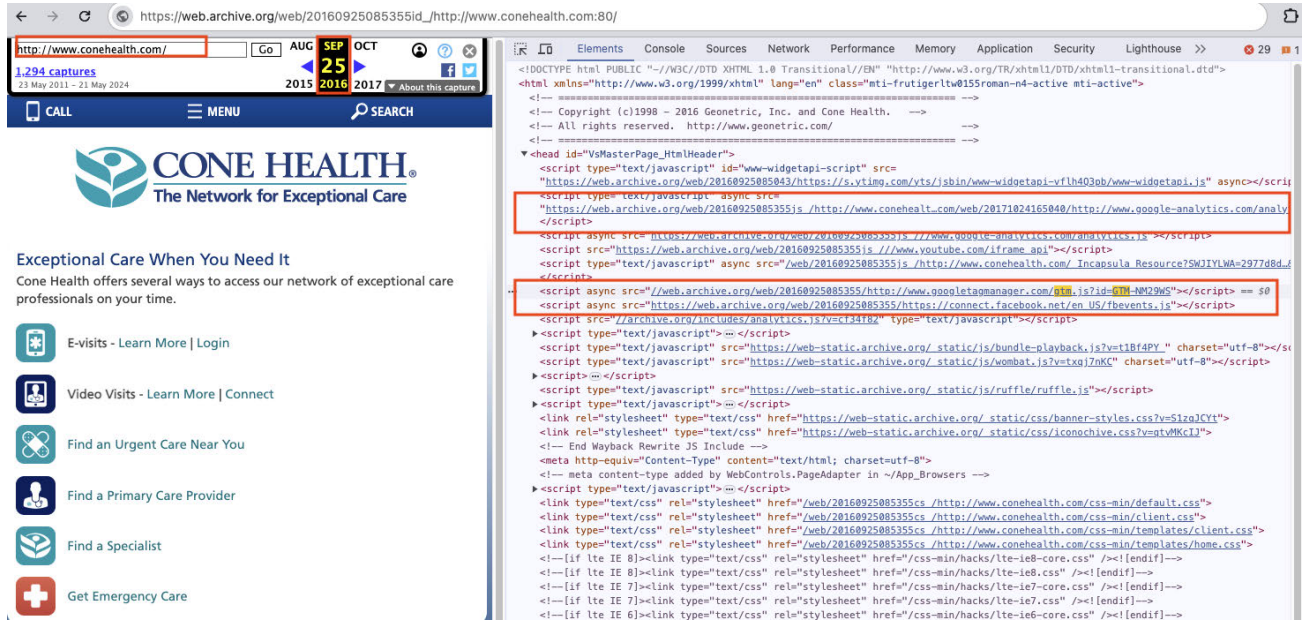


184. Archives of UA1's and GTM1's configuration files demonstrate the actions that Cone Health took using the Google tracking code that it installed and the custom events that it set up to transmit patients' Private Information to Google.

185. Using the Google tracking code installed on its Web Properties, Cone Health transmitted PageView and DoubleClick events about Users' activities. Upon a User's arrival on

48

Cone Health's homepage, Cone Health immediately sent a of PageView and Doubleclick event to Google revealing that the user was on the page, https://www.conehealth.com/. As Users navigated beyond the homepage, Cone Health continued to disclose user data including Users': (i) keyword, location, and physician searches, (ii) appointment scheduling activities, (iii) review of Cone Health services and events, and (iv) other activities that reveal their patient status.

186. Cone Health's disclosures of User's keyword searches begins as the search results page loads, immediately triggering the PageView event. As the page loads, Cone Health sends Google the website URL, including the title of the webpage visited.

187. Cone Health then discloses the User's activities as they interact with their search results. For instance, the User could click to view a physician's page, call a physician or book an appointment. As the User clicked for each action, Cone Health sent further PageView events revealing the User's action and the context of the User's search for doctors in Greensboro, North Carolina.

188. The User could then browse and click through their filtered search results to learn more and conduct activities such as book appointments. Cone Health disclosed details as Users performed these actions.

I. *Evidence That Cone Health Disclosed Users' Appointment Activities to Meta and Google*

189. When a User clicked to schedule an appointment, Cone Health transmitted a SubscribedButtonClick event to Facebook as well as Inbound Link and User Engagement events to Google:

49

Get Care Now | Cone Health

conehealth.com/patients-visitors/make-an-appointment/

CONE HEALTH.

Home » Patient & Family Resources » Get Care Now

**Get Care Now**

Save time and money by choosing the right care for you and your family.

Virtual Care — For non-emergency medical conditions, connect any

Primary Care — Schedule with a primary care provider for preventative care, general

Urgent Care — For non-emergency injuries or illnesses when your doctor's

---

Elements   Console   Sources   Network   Performance   Memory   Application

Preserve log   Disable cache   No throttling

Facebook   Invert   Hide data URLs   Hide extension URLs

All   Fetch/XHR   Doc   CSS   JS   Font   Img   Media   Manifest   WS   Wasm   Other   Blocked response cookies   Blocked requests

3rd-party requests

Headers   Payload   Preview   Response   Initiator   Timing   Cookies

**▼Query String Parameters**        view source        view URL-encoded

id: 707716599896829

ev: SubscribedButtonClick

dl: https://www.conehealth.com/wellness-matters/#LungCancer

rl: https://www.conehealth.com/services/cancer-care/what-you-should-know-about-lung-cancer-plus-two-womens-stories/

if: false

ts: 1716057344826

cd[buttonFeatures]: {"classList":"FullSizeButton","destination":"https://www.conehealth.com/patients-visitors/make-an-appointment/","id":"","imageUrl":"","innerText":"Need Care?\n\nMake an appointment.","numChildButtons":0,"tag":"a","name":""}

cd[buttonText]: Need Care?

Make an appointment.

cd[formFeatures]: [{"id":"__EVENTTARGET","name":"__EVENTTARGET","tag":"input","inputType":"hidden","valueMeaning":"empty"},{"id":"__EVENTARGUMENT","name":"__EVENTARGUMENT","tag":"input","inputType":"hidden","valueMeaning":"empty"},{"id":"__VIEWSTATE","name":"__VIEWSTATE","tag":"input","inputType":"hidden"},{"id":"__VIEWSTATEGENERATOR","name":"__VIEWSTATEGENERATOR","tag":"input","inputType":"hidden"}]

cd[pageFeatures]: {"title":"\n\tWellness Matters – Cone Health\n"}

cd[parameters]: []

190.    These events inform Google and Facebook that the User clicked "Need Care? Make an appointment".

191.　Cone Health also offered a more generalized appointment booking function on its website. Cone Health informed Google and Facebook about Users' appointment activities there as well.

192.　When a User clicked to "Make an Appointment" on Cone Health's website, Cone Health sent a pair of PageView and Microdata events divulging to Facebook that the User clicked "Make an Appointment.":
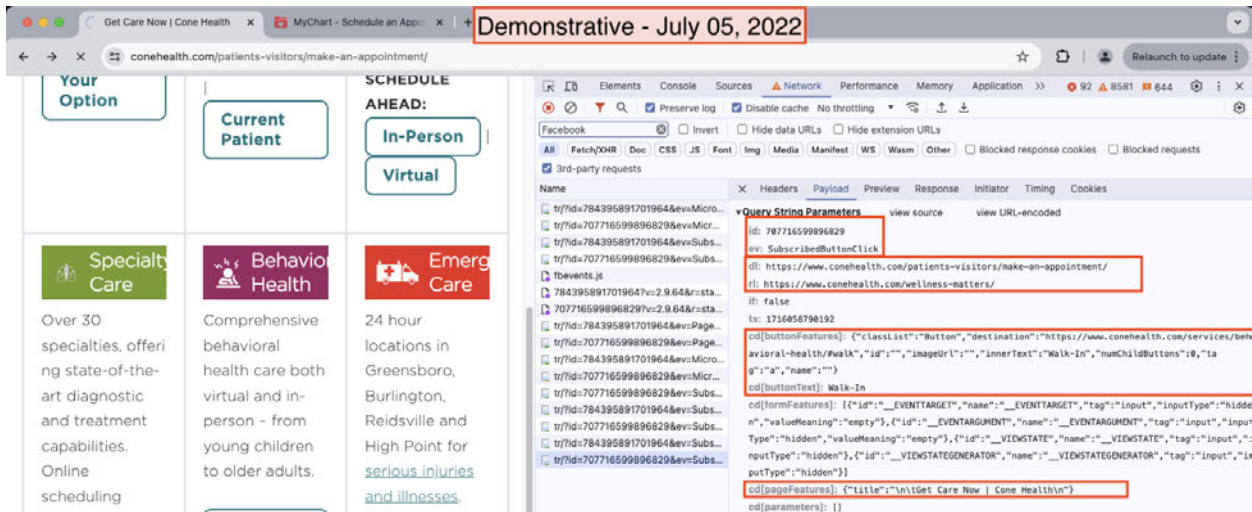
193.    As the User proceeded through the options to request appointments for Cone Health's different practices, such as virtual visits, primary care, or behavioral health, Cone Health would continue to share details about the user's activity with Google and Facebook. For example, as the User clicked to learn about walk-in appointments for Behavioral Health, Cone Health would report the User's activity by sending an Inbound Link event to Google and a SubscribedButtonClick event to Facebook:



54

*J.* ***Evidence That Cone Health Disclosed Users' Activities to Meta and Google As They Sought to Access Their Medical Records***

194. Upon a User's click to access the Medical Records page, Cone Health would send

a SubscribedButtonClick event informing Facebook about this activity:
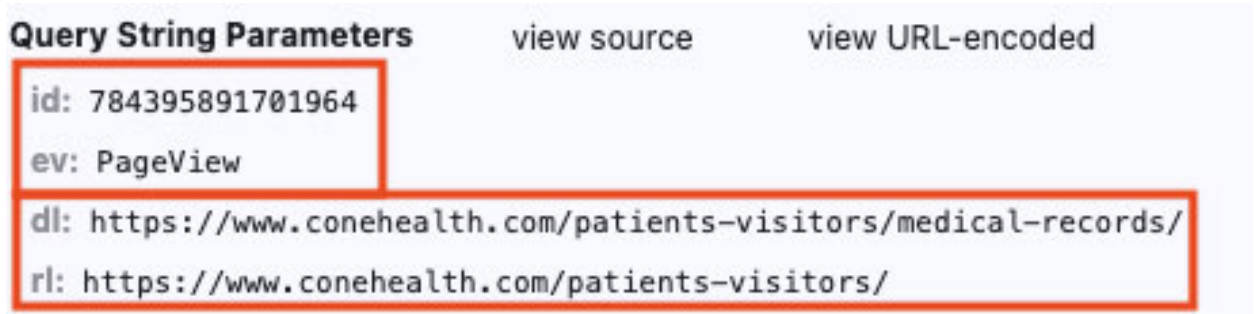
56

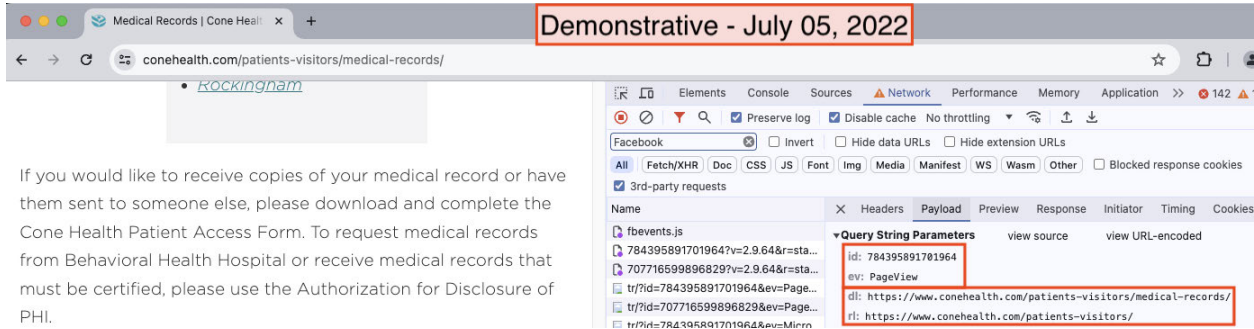195.    As the Medical Records page loaded, Cone Health would transmit a pair of PageView and Microdata events, revealing that the user was informed that they could use Cone Health's website to "gain secure, real-time access to your complete Cone Health Medical Records.":

If you would like to receive copies of your medical record or have them sent to someone else, please download and complete the Cone Health Patient Access Form. To request medical records from Behavioral Health Hospital or receive medical records that must be certified, please use the Authorization for Disclosure of PHI.

There is no charge to have your medical records sent to another healthcare provider. For other requests, fees may apply. Allow up 10-14 business days to receive copies of your medical records after receipt of your written request.

▼**Query String Parameters**    view source    view URL-encoded

id: 784395891701964

ev: Microdata

dl: https://www.conehealth.com/patients-visitors/medical-records/

rl: https://www.conehealth.com/patients-visitors/

if: false

ts: 1716060577645

cd[DataLayer]: []

cd[Meta]: {"title":"\n\tMedical Records | Cone Health\n","meta:keywords":"electronic records, meaningful use, patient records, medical records, EMR, privacy, MyChart, my chart,","meta:description":"Through Cone HealthLink (EMR) & MyChart, you and your care team gain secure, real-time access to your complete Cone Health medical records."}

cd[OpenGraph]: {}

59

196.    The User could download a request and authorization form for their health information from the Medical Records page. When a User did so, Cone Health would inform Facebook about this activity via a SubscribedButtonClick event which reveals that the user clicked to download an "authorization-for-disclosure-of-phi-english-7-14.pdf.":

197.  Cone Health also disclosed information to Google about Users' medical records related activities. When a User clicked to navigate to the Medical Records page, Cone Health would send Inbound Link and Navigation events disclosing that the user clicked for "Medical Records." Next, Cone Health would send a pageview event as the Medical Records page loaded:

198.     Cone Health would report users' medical records page activities as well. When the user clicked to download a medical authorization form, Cone Health would send Download and Inbound Link events which disclose to Google that the user accessed the "Request & Authorization For Use / Disclosure of Protected Health Information" document:

## K. Evidence That Cone Health Disclosed Users' Patient Portal Activities & Bill Pay Activities to Meta and Google

199. Cone Health also disclosed User activities that reveal their status as current patients. Two examples of such activities are Users' Patient portal and bill pay activities.

200. Upon a User's loading of the Patient portal page, Cone Health sent Facebook a SubscribedButtonClick event that the User clicked to access Cone Health's "Billing & Insurance" page located at https://www.conhealth.com/patinet-svisitors/patient-financial-services:

conehealth.com/patients-visitors/patient-financial-services/

**CONE HEALTH.**

Home » Patient & Family Resources » Billing & Insurance

## Billing and Insurance

### Contact Us

Get answers to your questions about billing and financial assistance. Call Cone Health Patient Financial Services at **336-832-8014** or **866-479-8800** or send us a message through your Cone Health Wallet.

Count on Cone Health to make paying for your care as easy and convenient as possible.

After you return home from the hospital, you'll receive a statement of charges and bills from the hospital, your physician and others who provided medical services during your hospital stay.

### Financial Assistance

If you're concerned about your ability to pay your bill, learn about our options for financial assistance.

### Medicaid Eligible Patients

Beginning on December 1, 2023, you may be able eligible for health care coverage through Medicaid even if you did not qualify before. Cone Health accepts Medicaid for most services. Get the details.

### Patient Estimates and Charges

---

image/avif,image/webp,image/apng,image/svg+xml,image/*;*/*;q=0.8

gzip, deflate, br, zstd

en-US,en;q=0.9

no-cache

sb=AEZ_ZXpz3WEvIUuWRO4NcH6N; datr=AEZ_ZbJ3fuYJCmfA_l8pfz-f;

ps_n=1; c_user=10[redacted]2; cpr=1;

xs=9%3AcROMAFWFgvBRcg%3A2%3A1713819308%3A-1%3A-

201.    Cone Health similarly informed Google that the user visited this page via a pair of

Inbound Link and Navigation events:

202.     When the User clicked to pay their medical bill online, Cone Health sent another

SubscribedButtonClick event to Facebook informing the User clicked a button labeled "Sign into

your Cone Health Wallet":

203.    Cone Health similarly informed Google of this via an Outbound Link event:

204.    Cone Health also disclosed users' patient portal activities to Google. When the login page loaded, Cone Health would transmit a pageview event to inform Google that the user was on the "MyChart - Login Page.":





68

205.    When new patients would go to sign up for a patient portal account, Cone Health

would send a pageview event revealing that the user was on the "MyChart – Choose a Signup

Method" page:
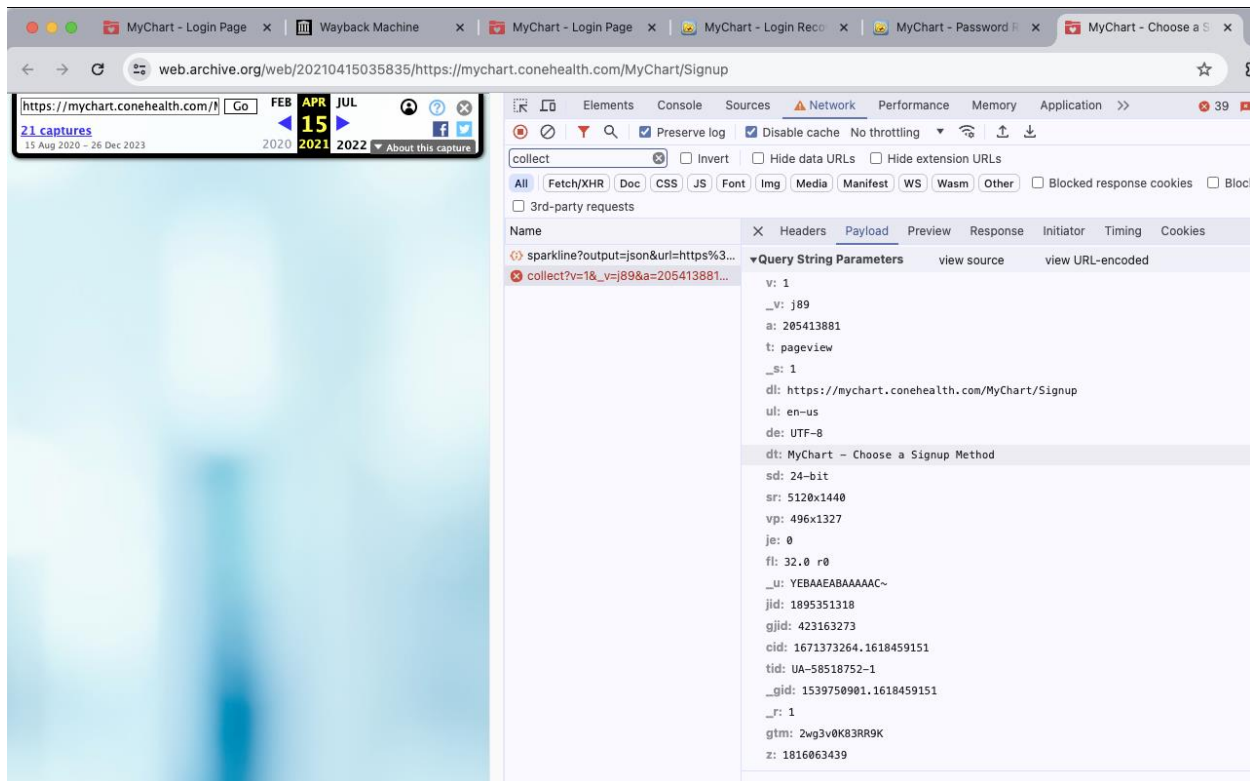
206.     Cone Health would also send pageview events revealing when users used either

the "MyChart – Password Reset Page" or the "MyChart – Login Recovery Page" pages:

## Query String Parameters    view source    view URL-encoded

```
v: 1
_v: j39
a: 1726971589
t: pageview
_s: 1
dl: https://mychart.conehealth.com/MyChart/recoverlogin.asp
ul: en-us
de: windows-1252
dt: MyChart - Login Recovery Page
sd: 24-bit
sr: 5120x1440
vp: 511x1312
je: 0
fl: 32.0 r0
_u: AEAAAEABI~
jid: 1986357934
cid: 701918424.1443931953
tid: UA-58518752-1
_r: 1
z: 1534279855
```

71

*L. Evidence That Cone Health Installed Third-Party Tracking Software Inside its Patient Portal Patient Portal*

207.     Plaintiff's investigation to-date revealed that Cone Health has been tracking patients' activities even *inside its patient portal*. Specifically, Cone Health embedded Google Tag Manager ("GTM"), a Google tool for installing and managing tracking codes, inside its patient portal.

208.     Discovery will help establish what specific tracking software Cone Health installed inside the patient portal and what information Cone Health was sharing with third parties via this software (in addition to the Meta Pixel on its Login and Pay Your Bill pages which revealed users' patient status to Facebook and likely other third parties).[64]

209.     The tracking software that can be installed on a website using GTM include the Meta Pixel, Google Analytics and other Google marketing products.[65]

210.     To date, Plaintiff's investigation reveals that at least one of the trackers Cone Health installed in a GTM on the patient portal is the Google Universal Analytics tracker, a category of tracker that discloses to Google a user's unique IP address.

*M.     Cone Health's Privacy Policies & Promises.*

211.     Cone Health's privacy policies represent to Plaintiff and Class Members that Cone Health will keep Private Information private and confidential, and it will only disclose Private Information under certain circumstances.

---

[64] Google Tag Manager is used for managing and deploying marketing tags (tracking software) on a website without having to modify the code. *See* https://www.semrush.com/blog/google-tag-manager/

[65] *Id*.

72

212.    Cone Health publishes several privacy policies that represent to Users that Cone Health will keep sensitive information confidential and that it will only disclose PII and PHI provided to it under certain circumstances, none of which apply here.[66]

213.    Cone Health's separate Notice of Privacy Practices assures Plaintiff and Class Members that Cone Health is "required by law to make sure that health information that identifies you is kept private". [67]

214.    Cone Health's Notice of Privacy Practices explains Cone Health's duties with respect to IIHI and the exceptions for when Cone Health can use and disclose Plaintiff's and Class Members' PHI in the following ways:

- For Treatment;
- For Payment;
- For Health Care Operations;
- Treatment Alternatives;
- Triad HealthCare Network;
- Data Sharing;
- Fundraising Activities;
- The Directory;
- Individuals Involved in Your Care or Payment for Your Care;
- Research;
- As Required or Permitted By Law;
- To Avert a Serious Threat to Health or Safety;
- Organ and Tissue Donation;
- Workers' Compensation;
- Public Health Risks;
- Health Oversight Activities;
- Lawsuits and Disputes;
- Law Enforcement;
- Coroners, Medical Examiners and Funeral Directors;
- Security, Intelligence Activities and Protective Services;
- Inmates;
- Behavioral Health Care;

---

[66]https://www.conehealth.com/patients-visitors/privacy/notice-of-privacy-practices/ (last visited May 31, 2024).

[67] *Id.*

73

- Minors.[68]

215.    Cone Health's privacy policy does not permit Cone Health to use and disclose Plaintiff's and Class Members' IIHI for marketing purposes. Cone Health promise patients that "All other information that is shared in a way not addressed in this notice, **including uses or disclosures for marketing purposes**, or disclosures of your information in exchange for some form of payment, will be made only after you give your written permission or as required by law."[69] (emphasis added)

216.    Notwithstanding these representations, Cone Health installed Google Analytics and Meta's Collection Tools on its Web Properties and, thereafter, began to automatically transmit extensive IIHI from everyone who visited its Web Properties to Google and Meta.

217.    After receiving IIHI communicated on Cone Health's Web Properties, Google and Meta analyze and use this information for their own commercial purposes that include building more fulsome profiles of its Users' preferences and traits and selling targeted advertisements based on this information. Google and Meta also receive an additional commercial benefit from Cone Health's use of the Google and Meta Collection Tools, namely that it provides Cone Health with a greater incentive to advertise on Google and Meta's platforms.

218.    After receiving IIHI communicated on Cone Health's Web Properties, Google and Meta forward this data, and its analysis of this data, to Cone Health. Cone Health then uses this data and analysis for its own commercial purposes that include understanding how Users use its Website and determining what ads Users see on its Website.

---

[68] *Id*.

[69] *Id.*

74

219. At all times relevant to this Complaint, Cone Health did not notify Users that it automatically sends IIHI communicated on its Web Properties to Google and Meta.

220. At all times relevant to this Complaint, Cone Health did not notify Users of its Web Properties that IIHI they communicate on its Web Properties were being used by Google and Meta for commercial purposes.

221. At all times relevant to this Complaint, Cone Health did not notify Users of its Web Properties that it was using the IIHI they communicate on its Web Properties for commercial purposes.

222. Neither Google nor Meta has secured any informed consent or written permission allowing them to use IIHI communicated on Cone Health's Web Properties for commercial purposes.

223. Cone Health has not secured any informed consent or written permission allowing it to share IIHI communicated on its Web Properties with Google or Meta or for commercial purposes.

224. Cone Health violated its own privacy policy by unlawfully intercepting and disclosing Plaintiff's and Class Members' Private Information to Facebook and third parties without adequately disclosing that it shared Private Information with third parties and without acquiring the specific patients' consent or authorization to share the Private Information.

*N.* ***Cone Health's Conduct Violates Federal & State Privacy Laws.***

*1. The HIPAA Privacy Rule Protects Patient Healthcare Information.*

225. Patient healthcare information in the United States is protected by federal law under HIPAA and its implementing regulations, which are promulgated by HHS.

75

226.    The HIPAA Privacy Rule, located at 45 C.F.R. § 160 and 45 C.F.R. § 164 (A) and (E): "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically."[70]

227.    The Privacy Rule broadly defines PHI as "individually identifiable health information" 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.

228.    IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare 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.

229.    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:

---

[70] The HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (last visited Jun. 19, 2024).

a. Names;

b. Medical record numbers;

c. Account numbers;

d. Device identifiers and serial numbers;

e. Web Universal Resource Locators (URLs);

f. Internet Protocol (IP) address numbers; … and

g. 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 subject of the information." 45 C.F.R. § 164.514.

230. The HIPAA Privacy Rule requires any "covered entity"—which includes healthcare providers like Cone Health—to maintain appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of PHI without authorization. 45 C.F.R. §§ 160.103, 164.502.

231. An individual or corporation violates the HIPAA Privacy Rule if it knowingly: "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually-identifiable health information relating to an individual." The statute states that a "person … shall be considered to have obtained or disclosed individually-identifiable health information … if the information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization."  42 U.S.C. § 1320(d)(6).

232. The criminal and civil penalties imposed by 42 U.S.C. § 1320(d)(6) apply directly to Cone Health when it is knowingly disclosing IIHI relating to an individual, as those terms are defined under HIPAA.

233.    Violation of 42 U.S.C. § 1320(d)(6) is subject to criminal penalties 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. § 1320(d)(6)(b). In such cases, an entity that knowingly obtains IIHI relating to an individual "shall be fined not more than $250,000, imprisoned not more than 10 years, or both."  42 U.S.C. § 1320(d)(6)(b)(1).

   *2.  HIPAA Protects Patient Status Information.*

234.    HIPAA also protects against revealing an individual's status as a patient of a healthcare provider.

235.    Guidance from HHS confirms that HIPAA protects patient status:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data.… **If such information was listed with health condition, healthcare provision or payment data, such as an indication that an individual was treated at a certain clinic, then this information would be PHI.**[71]

236.    HHS's guidance for marketing communications states that healthcare providers may not provide patient lists for marketing purposes without the consent of every included patient:

> 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**

---

[71] Office for Civil Rights, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* at 5 (emphasis added) (Nov. 26, 2012), https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html.

78

**sell lists of patients to third parties without obtaining authorization from each person on the list.**[72]

237.    HHS has previously instructed that the HIPAA Privacy Rule protects patient status:

a.  "The sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);

b.  "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);

c.  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); and

d.  The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1). Even then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R. § 164.510(2).

*3.  HIPAA's Protections Do Not Exclude Internet Marketing.*

238.    As OCR reminded entities regulated under HIPAA (like Cone Health) in its recently issued *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* bulletin:

> Regulated 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. ***For example, disclosures of PHI to tracking technology vendors for***

---

[72]    Marketing, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html

79

*marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.*[73]

239. OCR makes it clear that information that is routinely collected by vendors on public-facing websites may be PHI including, but not limited to, unique identifiers such as IP addresses, device IDs or email addresses.[74]

240. Further, HIPAA applies to healthcare providers' webpages with tracking technologies even outside the patient portal, *i.e.*, to "unauthenticated" webpages:

> [T]racking technologies on unauthenticated webpages may 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 permit[] individuals to 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 healthcare provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.[75]

241. **The HHS bulletin reminds covered entities, like Cone Health, of their long-standing duty to safeguard PHI**, explicitly noting that "it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors," and proceeding to explain how online tracking technologies violate the same HIPAA privacy rules that have existed for decades.[76]

---

[73] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* (emphasis added) (updated March 18, 2024) (last visited Jun. 19, 2024).

[74] *See id*.

[75] *Id.*

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

242. Disclosures of PHI for online marketing or sales purposes require patient authorization under HIPAA, which Cone Health did not obtain here. *See* 45 CFR § 164.508(a)(3) ("a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of: (A) a face-to-face communication made by a covered entity to an individual; or (B) a promotional gift of nominal value provided by the covered entity."); 45 CFR § 164.508(a)(4) ("a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined in § 164.501 of this subpart [and] [s]uch authorization must state that the disclosure will result in remuneration to the covered entity.").

243. As a result, a healthcare provider like Cone Health may not disclose PHI to a tracking technology vendor, like Meta or Google, unless it has properly notified Website Users and entered into a business associate agreement with the vendor in question.

244. Yet Cone Health disclosed Plaintiff's and Class Members' PHI without their consent and without a business associate agreement with Meta or Google.

*4. Under HIPAA, IP Addresses are Personally Identifiable Information.*

245. Through the use of the Google and Meta Collection Tools, computer IP addresses are among the Private Information that was improperly disclosed to Facebook.

246. An IP address is a number that identifies the address of a device connected to the Internet.

247. IP addresses are used to identify and route communications on the Internet.

248. IP addresses of individual Internet users are used by Internet service providers, websites, and third-party tracking companies to facilitate and track Internet communications.

249. Facebook tracks every IP address ever associated with a Facebook user.

81

250. Google also tracks IP addresses associated with Internet users.

251. Facebook, Google, and other third-party marketing companies track IP addresses for use of tracking and targeting individual homes and their occupants with advertising by using IP addresses.

252. Under HIPAA, an IP address is considered PII:

    a. HIPAA defines PII to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).

    b. HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the 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).

253. Consequently, by disclosing Plaintiff's and Class Members' IP addresses along with making their healthcare appointments, paying their medical bills or logging into (or using) the patient portal for their medical care, Cone Health's business practices violated HIPAA and industry privacy standards.

      *5. The FTC Act Protects Health Information.*

254. The FTC has made clear that "health information" is "anything that conveys information—or enables an information—about a consumer's health" and provides an example that location-data alone (such as repeated trips to a cancer treatment facility") "may convey highly sensitive information about a consumer's health."[77]

---

[77] Jillson, Elisa, *Protecting the privacy of health information: A baker's dozen takeaways from FTC cases*, Federal Trade Commission (July 25, 2023), https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases.

82

255.    The FTC joined HHS in notifying HIPAA-covered entities and non-HIPAA-covered entities that sharing such "health information" with Google and Facebook is an unfair business practice under federal law:

> When consumers visit a hospital's website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers' health information from potential misuse and exploitation."[78]

256.    While the OCR's guidance on some of these topics was vacated in part due to improper rulemaking, the *FTC's* guidance on these topics remains unchanged and its enforcement actions remain in effect and highly instructive.

### 6.    *Cone Health Violated Industry Standards.*

257.    A medical provider's duty of confidentiality is embedded in the physician-patient and hospital-patient relationship, it is a cardinal rule.

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

259.    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)

---

[78] *FTC and HHS Warn Hospital Systems and Telehealth Providers About Privacy and Security Risks from Online Tracking Technologies*, Federal Trade Commission (July 20, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking.

260.   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.

261.   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.

## O.   *Plaintiff's & Class Members' Expectations of Privacy.*

262.   Plaintiff and Class Members were aware of Cone Health's duty of confidentiality

when they sought medical services from Cone Health.

263.   Indeed, at all times when Plaintiff and Class Members provided their PII and/or

PHI to Cone Health, they each had a reasonable expectation that the information would remain

private and that Cone Health would not share their Private Information with third parties for a

commercial purpose, unrelated to patient care.

264.   Privacy polls and studies show that the overwhelming majority of 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.

84

265.    For example, a recent Consumer Reports study shows that 92% of Americans believe that 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.[79]

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

267.    Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information are grounded in, among other things, Cone Health's status as a healthcare provider, Cone Health's common law obligation to maintain the confidentiality of patients' Private Information, state and federal laws protecting the confidentiality of medical information, state and federal laws protecting the confidentiality of communications and computer data, state laws prohibiting the unauthorized use and disclosure of personal means of identification, and Cone Health's express and implied promises of confidentiality.

### P.    *Patients Have Protectable Property Interests in Their IIHI.*

268.    Property is the right of any person to possess, use, enjoy or dispose of a thing, including intangible things like data and communications. Plaintiff and Class Members have a vested property right in their IIHI.

269.    Federal and state laws grant patients the right to protect the confidentiality of data that identifies them as patients of a particular healthcare provider and restrict the use of their health

---

[79] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, (May 11, 2017), available at https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/ (last visited Apr. 19, 2024).

data, including their status as a patient, to only uses related to their care or otherwise authorized by federal or state law in the absence of patient authorization.

270. A patient's right to protect the confidentiality of their health data and restrict access to this data is valuable.

271. In addition, patients enjoy property rights in the privacy of their health communications under statutes such as HIPAA. State health privacy laws and American courts have also long recognized common law property rights in the content of a person's communications that are not to be used or disclosed to others without authorization.

272. Property rights in communications and information privacy are established by:

    a. The Electronic Communications Privacy Act, including Title I (the Wiretap Act); Title II (the Stored Communications Act); and Title III (the Pen Register Act); and

    b. Common law information property rights regarding the exclusive use of confidential information that have existed for centuries and continue to exist, s*ee Folsom v. Marsh*, 9 F.Cas. 342, 346 (C.C.D. Mass. 1841) (Story, J); *Baker v. Libbie*, 210 Mass. 599, 602 (1912); *Denis v. LeClerc*, 1 Mart. (La.) 297 (1811).

273. Meta's CEO, Mark Zuckerberg, has acknowledged that Meta users have an ownership interest in their data. In 2010, when Meta first revealed its "Download Your Information" tool, Zuckerberg stated that, "People own and have control over all info they put into Facebook and 'Download Your Information' enables people to take stuff with them."[80] Although Zuckerberg's statements regarding people's ability to "control" the information "put into Facebook" and the ability to access all such data via DYI is not true, his statement about data ownership is true.

---

[80] https://techcrunch.com/2010/10/06/facebook-now-allows-you-to-download-your-information/.

274. Cone Health's unauthorized interception and disclosure of Plaintiff's and Class Members' IIHI violated their property rights to control how their data and communications are used and who may be the beneficiaries of their data and communications.

*Q. The Information Cone Health Discloses to Google and Meta Without Plaintiff's or Class Members' Consent Has Actual, Measurable Monetary Value.*

275. After receiving IIHI communicated on Cone Health's Web Properties, both Google and Meta forward their analysis of this data to Cone Health. Cone Health then uses that analysis for its own commercial purposes, including to target ads at existing patients or other people with characteristics similar to certain groups of Users.

276. Technology companies are under particular 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.

277. Meta "generate[s] substantially all of [its] revenue from advertising."[81]

278. Meta annually receives billions of dollars of unearned advertising sales revenue from Meta healthcare Partners, including Google, who are targeting Facebook users based on their health information.

279. Similarly, Google a vast majority of its revenue from advertising. Google annually receives billions of dollars of unearned advertising sales revenue from Google healthcare Partners who target Google users based on their health information.

---

[81] Meta 2022 Annual Report at 17.

280. The robust market for Internet user data has been analogized to the "oil" of the tech industry.[82] A 2015 article from TechCrunch accurately noted that "[d]ata has become a strategic asset that allows companies to acquire or maintain a competitive edge."[83]

281. That article noted that the value of a single Internet user—or really, a single user's data—varied from about $15 to more than $40.

282. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data (after costs).[84] At the time, estimates for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.

283. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes: "Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information."[85]

284. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis and use. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiff herein can sell or

---

[82] *See* https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last visited Apr. 19, 2024).

[83] *See* https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/ (last visited Jan. 9, 2024).

[84] *See What Your Data is Really Worth to Facebook* (Jul. 12, 2019), https://washingtonmonthly.com/2019/07/12/what-your-data-is-really-worth-to-facebook/ (last visited Apr. 19, 2024).

[85] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056-57 (2004).

monetize their own data. For example, Nielsen Data and Mobile Computer will pay Internet users for their data.[86]

285.   There are countless examples of this kind of market, which is growing more robust as information asymmetries are diminished through revelations to users as to how their data is being collected and used.

286.   Courts recognize the value of personal information and the harm when it is disclosed without consent. *See, e.g., In re Facebook Privacy Litig.*, 572 F. App'x 494, 494 (9th Cir. 2014) (holding that plaintiffs' allegations that they were harmed by the dissemination of their personal information and by losing the sales value of that information were sufficient to show damages for their breach of contract and fraud claims); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (recognizing "the value that personal identifying information has in our increasingly digital economy").

287.   Healthcare data is particularly valuable on the black market because it often contains all of an individual's PII and medical conditions as opposed to a single piece of information that may be found in a financial breach.

288.   Healthcare data is incredibly valuable because, unlike a stolen credit card that can be easily canceled, most people are unaware that their medical information has been sold. Once it has been detected, it can take years to undo the damage caused.

289.   The value of health data is well-known and various reports have been conducted to identify its value.

---

[86] *See 10 Apps for Selling Your Data for Cash*, https://wallethacks.com/apps-for-selling-your-data/ (last visited Jan. 9, 2024).

290.     Specifically, in 2023, the Value Examiner published a report entitled Valuing Healthcare Data. The report focused on the rise in providers, software firms and other companies that are increasingly seeking to acquire clinical patient data from healthcare organizations. The report cautioned providers that they must de-identify data and that purchasers and sellers of "such data should ensure it is priced at fair market value to mitigate any regulatory risk."[87]

291.     Trustwave Global Security published a report entitled The Value of Data. With respect to healthcare data records, the report found that they may be valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[88]

292.     The value of health data has also been reported extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry," in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[89]

293.     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."[90]

---

[87]                                                                                          *See* https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf (last visited Apr. 19, 2024).

[88] *See* https://www.imprivata.com/blog/healthcare-data-new-prize-hackers (last visited Jan. 9, 2024)                                              (citing                                              https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf).

[89] *See* https://time.com/4588104/medical-data-industry/ (last visited Apr. 19, 2024).
[90]     *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited Apr. 19, 2024).

294.     The dramatic difference in the price of healthcare data compared to other forms of private information commonly sold is evidence of the value of PHI.

295.     These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users' stolen data, surely Internet users can sell their own data.

296.     In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

### R. Cone Health was Enriched & Benefitted from the Use of The Google & Meta Collection Tools & Unauthorized Disclosures.

297.     Cone Health installed the Google and Meta Collection Tools on the Web Properties to benefit its own marketing and revenue.

298.     In exchange for disclosing the PII of its patients, Cone Health is compensated by Google and Facebook in the form of enhanced advertising services and more cost-efficient marketing.

299.     Retargeting is a form of online marketing that targets users with ads based on their previous Internet communications and interactions. In particular, retargeting operates through code and tracking pixels placed on a website and cookies to track website visitors and then places ads on other websites the visitor goes to later.[91]

300.     The process of increasing conversions and retargeting occurs in the healthcare context by sending a successful action on a healthcare website back to Google and Facebook via the tracking technologies and the Google and Meta Collection Tools embedded on, in this case,

---

[91] *The complex world of healthcare retargeting,* https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/ (last visited Apr. 19, 2024).

91

Cone Health's Web Properties. For example, when a User searches for doctors or medical conditions or treatment on Cone Health's Web Properties, that information is sent to Facebook. Facebook can then use its data on the User to find more users to click on a Cone Health ad and ensure that those Users targeted are more likely to convert.[92]

301.    Through this process, the Google and Meta Collection Tools load and captures as much data as possible when a User loads a healthcare website that has installed the Google and Meta Collection Tools. The information the Google and Meta Collection Tools capture, "includes URL names of pages visited, and actions taken—all of which could be potential examples of health information."[93]

302.    Plaintiff's and Class Members' Private Information has considerable value as highly monetizable data especially insofar as it allows companies to gain insight into their customers so that they can perform targeted advertising and boost their revenues.

303.    In exchange for disclosing the Private Information of their account holders and patients, Cone Health is compensated in the form of enhanced advertising services and more cost-efficient marketing on its platform.

---

[92] *See, e.g.*, *How to Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking* (Mar. 14, 2023), *https://www.freshpaint.io/blog/how-to-make-facebook-ads-hipaa-compliant-and-still-get-conversion-tracking* (last visited Apr. 19, 2024).

[93] *Id.*

92

304. But companies have started to warn about the potential HIPAA violations associated with using pixels and tracking technologies because many such trackers are not HIPAA-compliant or are only HIPAA-compliant if certain steps are taken.[94]

305. For example, Freshpaint, a healthcare marketing vendor, cautioned that "Meta isn't HIPAA-compliant. They don't sign BAAs, and the Meta Pixel acts like a giant personal user data vacuum sending PHI to Meta servers," and "[i]f you followed the Facebook (or other general) documentation to set up your ads and conversion tracking using the Meta Pixel, remove the Pixel now."[95]

306. Meta's Terms of Service, Data Policy, and Cookies Policy neither inform Facebook users that Meta may acquire their health information when they interact with healthcare providers' websites and applications, nor obtain their consent for any such acquisitions.

307. Google's Terms of Service, Data Policy, and Cookies Policy neither inform Google users that Google may acquire their health information when they interact with healthcare providers' websites and applications, nor obtain their consent for any such acquisitions.

308. Medico Digital also warns that "retargeting requires sensitivity, logic and intricate handling. When done well, it can be a highly effective digital marketing tool. But when done badly, it could have serious consequences."[96]

309. Whether a User has a Facebook profile is not indicative of damages because Facebook creates shadow profiles, and at least one court has recognized that the Meta Pixel's

---

[94] *See The guide to HIPAA compliance in analytics,* https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf (explaining that Google Analytics 4 is not HIPAA-compliant) (last visited Jan. 9, 2024).

[95] *How To Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking*, *supra,* n.92.
[96] *The complex world of healthcare retargeting, supra,* n.91.

93

ability to track comprehensive browsing history is also relevant. *See, e.g.*, *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1078–79 (N.D. Cal. 2021) (finding a reasonable expectation of privacy where Google combined the unique identifier of the user it collects from websites and Google Cookies that it collects across the internet on the same user).[97]

310. Upon information and belief, as part of its marketing campaign, Cone Health re-targeted patients and potential patients to get more patients connected to the Cone Health Patient portal.

311. By utilizing the Google and Meta Collection Tools, the cost of advertising and retargeting was reduced, thereby benefiting Cone Health.

## REPRESENTATIVE PLAINTIFF EXPERIENCE

### A. *Plaintiff Ashika Singh*

312. Plaintiff Ashika Singh entrusted her Private Information to Cone Health. As a condition of receiving Cone Health's services, Plaintiff disclosed her Private Information to Cone Health.

313. On numerous occasions, from at least 2006 to present, Plaintiff accessed Cone health patient portal and Cone Health's Website on her mobile device and/or computer to receive healthcare services from Cone Health and at Cone Health's direction.

314. Plaintiff used Cone Health's Web Properties, including Cone Health's Patient Portal, multiple times per year to, among other things, make appointments with doctors, exchange messages with her doctors, fill out questionnaires requested by her doctors, request referrals for

---

[97] *See* Facebook Shadow Profiles (February 2022), https://www.cesifo.org/DocDL/cesifo1_wp9571.pdf

specific health issues, ███████████████████████████████████████

███████

315.    Plaintiff has been in ███████████████████████████████

████████████████████████████████████████████████████████

█████████████████. Plaintiff submitted information to Cone Health's Web Properties about

each of these medical conditions. For example, in May 2024, Plaintiff exchanged messages on

Cone Health's Web Properties about ██████████████████████████████

███████████.

316.    Plaintiff has used Cone Health's Web Properties to send messages to ██████

████████████████████████████████████████████████████████

██████.

317.    Plaintiff has used and continues to use the same devices to maintain and access both

an active Google account and an active Facebook account throughout the relevant period in this

case.

318.    Plaintiff read Cone Health's Notice of Privacy Practices concerning the

circumstances under which Cone Health would share her health information when she first became

a patient of Cone Health and each time the policy was presented for her to read and sign.

319.    Plaintiff provided her Private Information to Cone Health and trusted that the

information would be safeguarded according to Cone Health's policies and state and federal law.

320.    Plaintiff reasonably expected that her communications with Cone Health via the

Web Properties were confidential, solely between herself and Cone Health, and that such

communications would not be transmitted to or intercepted by a third party.

95

321. Pursuant to the systematic process described herein, Cone Health assisted Google and Meta with intercepting Plaintiff's communications, including those that contained PII, PHI and related confidential information.

322. Cone Health transmitted to Google and Meta Plaintiff's Facebook ID or cid parameter cookie, computer IP address, and information relating to her medical conditions,
███████████

323. Cone Health assisted these interceptions without Plaintiff's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Cone Health breached confidentiality and unlawfully disclosed Plaintiff's PII and/or PHI.

324. Cone Health did not inform Plaintiff that it had shared her Private Information with Google and Meta.

325. Plaintiff suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of her Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages and (vi) the continued and ongoing risk to her Private Information.

326. Plaintiff is an active patient of Cone Health and seeks to continue to use the Web Properties to view her test results and communicate other Private Information concerning her medical conditions with Cone Health, but fears that without court action, her Private Information will be shared with unauthorized third parties, such as Google and Meta, in the future.

327. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Cone Health's possession, is protected and safeguarded from future unauthorized disclosure.

96

## TOLLING

328. Any applicable statutes of limitation have been tolled by Cone Health's knowing and active concealment of its incorporation of the Google and Meta Collection Tools into its Web Properties.

329. The Google trackers Meta Pixels and other tracking tools on Cone Health's Web Properties were and are entirely invisible to a Web Properties visitor.

330. Through no fault or lack of diligence, Plaintiff and Class Members were deceived and could not reasonably discover Cone Health's deception and unlawful conduct.

331. Plaintiff was ignorant of the information essential to pursue her claims, without any fault or lack of diligence on her part.

332. Cone Health had exclusive knowledge that its Web Properties incorporated the Google trackers, Meta Pixels and other tracking tools and yet failed to disclose to its patients, including Plaintiff and Class Members, that by seeking medical care through Cone Health's Website, Plaintiff's and Class Members' Private Information would be disclosed or released to Google, Facebook, and other unauthorized third parties.

333. Under the circumstances, Cone Health was under a duty to disclose the nature, significance, and consequences of its collection and treatment of its patients' Private Information. In fact, to the present, Cone Health has not conceded, acknowledged, or otherwise indicated to its patients that it has disclosed or released their Private Information to unauthorized third parties. Accordingly, Cone Health is estopped from relying on any statute of limitations.

334. Moreover, all applicable statutes of limitation have also been tolled pursuant to the discovery rule.

97

335. The earliest that Plaintiff or Class Members, acting with due diligence, could have reasonably discovered Cone Health's conduct would have been shortly before the filing of this suit.

## CLASS ACTION ALLEGATIONS

336. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class") pursuant to Fed. R. Civ. P. 23.

337. The nationwide Class that Plaintiff seeks to represent is defined as follows:

> All persons residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Google Collection Tools and/or the Meta Collection Tools on Cone Health's Web Properties.

338. Excluded from the Class are Cone Health, its agents, affiliates, parents, subsidiaries, any entity in which Cone Health has a controlling interest, any Cone Health officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

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

340. **Numerosity, Fed. R. Civ. P. 23(a)(1):** The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are millions of individuals whose PII and PHI may have been improperly accessed by Google and Facebook, and the Class is identifiable within Cone Health's records.

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

98

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

b. Whether Cone Health had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

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

d. Whether Cone Health adequately, promptly and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;

e. Whether Cone Health violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

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

g. Whether Cone Health engaged in unfair, unlawful or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

h. Whether Cone Health violated the consumer protection statutes invoked herein;

i. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Cone Health's wrongful conduct;

j. Whether Cone Health knowingly made false representations as to its data security and/or Privacy Policy practices;

k. Whether Cone Health knowingly omitted material representations with respect to its data security and/or Privacy Policies practices; and

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

342. **Typicality, Fed. R. Civ. P. 23(a)(3):** Plaintiff's claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of Cone Health's incorporation of the Google and Meta Collection Tools, due to Cone Health's misfeasance.

343. **Predominance.** Cone Health engaged in a common course of conduct toward Plaintiff and Class Members, in that Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully disclosed in the same way. The common issues arising from

99

Cone Health's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy. Cone Health's policies challenged herein apply to and affect Class Members uniformly, and Plaintiff's challenge of these policies hinges on Cone Health's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

344. **Adequacy of Representation, Fed. R. Civ. P. 23(a)(4):** Plaintiff will fairly and adequately represent and protect the interests of Class Members in that Plaintiff has 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.

345. **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 a large number of 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 large corporations, like Cone Health. 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.

346.    **Policies Generally Applicable to the Class.** This class action is also appropriate for certification because Cone Health acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Cone Health's policies challenged herein apply to and affect Class Members uniformly, and Plaintiff's challenge of these policies hinges on Cone Health's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

347.    The nature of this action and the nature of laws available to Plaintiff and Class Members makes 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 Cone Health 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 was 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.

348.    The litigation of the claims brought herein is manageable. Cone Health'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.

349.    Adequate notice can be given to Class Members directly using information maintained in Cone Health's records.

101

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

351.    Further, Cone Health acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

352.    Likewise, particular issues under Fed. R. Civ. P. 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 particular issues include, but are not limited to:

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

     b.  Whether Cone Health owed a legal duty to not disclose Plaintiff's and Class Members' Private Information with respect to Cone Health's privacy policy;

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

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

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

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

102

**g.** Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Cone Health's wrongful conduct.

## CAUSES OF ACTION

## COUNT ONE

## VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
### 18 U.S.C. § 2511(1), *et seq.*
### Unauthorized Interception, Use and Disclosure
### (*On Behalf of Plaintiff & the Nationwide Class*)

353.   Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

354.   The ECPA prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

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

356.   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.

357.   The transmissions of Plaintiff's PII and PHI to Cone Health's Web Properties qualify as "communications" under the ECPA's definition of 18 U.S.C. § 2510(12).

358.   **Electronic Communications**. The transmission of PII and PHI between Plaintiff and Class Members and Cone Health's Web Properties 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 photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

103

359.    **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).

360.    Cone Health's intercepted communications include, but are not limited to, communications to/from Plaintiff and Class Members regarding PII and PHI, diagnosis of certain conditions, treatment/medication for such conditions, and scheduling of appointments.

361.    Furthermore, Cone Health intercepted the "contents" of Plaintiff's communications in at least the following forms:

    a.    The parties to the communications;

    b.    The precise text of patient search queries;

    c.    PII such as patients' IP addresses, Facebook IDs, cid parameter cookie, browser fingerprints, and other unique identifiers;

    d.    The precise text of patient communications about specific doctors;

    e.    The precise text of patient communications about specific medical conditions;

    f.    The precise text of information generated when patients requested or made appointments,

    g.    The precise text of patient communications about specific treatments;

    h.    The precise text of patient communications about scheduling appointments with medical providers;

    i.    The precise text of patient communications about billing and payment;

    j.    The precise text of specific buttons on Cone Health's Website that patients click to exchange communications including Log-Ins, Registrations, Requests for Appointments, Search, and other buttons;

    k.    The precise dates and times when patients click to Log-In on Cone Health's Web Properties;

     l.   The precise dates and times when patients visit Cone Health's Web Properties;

    m.  Information that is a general summary or informs third parties of the general subject of communications that Cone Health sends back to patients in response to search queries and requests for information about specific doctors, conditions, treatments, billing, payment, and other information.

362.    For example, Cone Health's interception of the fact that a patient views a webpage like:

https://www.conehealth.com/locations/profile/cone-health-cancer-center-at-alamance-regional/?searchId=20da3693-9f2d-ef11-a86b-000d3a61151d&sort=15

involves "content," because it communicates that patient's request for the information on that page.

363.    **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).

364.    **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.   The cookies Cone Health, Google, and Meta use to track Plaintiff's and the Class Members' communications;

    b.   Plaintiff's and Class Members' browsers;

    c.   Plaintiff's and Class Members' computing devices

    d.  Cone Health's web servers and

e. The Google and Meta Collection Tools, including the Meta Pixel and Google tracking code deployed by Cone Health to effectuate the sending and acquisition of patient communications.

365. By utilizing and embedding the Meta Pixel and Google tracking code on its Web Properties, Cone Health 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).

366. Specifically, Cone Health intercepted Plaintiff's and Class Members' electronic communications via the Meta Pixel and Google tracking code, which tracked, stored, and unlawfully disclosed Plaintiff's and Class Members' Private Information to third parties such as Facebook and Google.

367. Cone Health's intercepted communications include, but are not limited to, communications to/from Plaintiff and Class Members regarding PII and PHI, treatment, medication, and scheduling.

368. This information was, in turn, used by third parties, such as Facebook and Google to 1) place Plaintiff and Class Members in specific health-related categories and 2) target Plaintiff and Class Members with advertising associated with their specific health conditions.

369. 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), Cone Health violated 18 U.S.C. § 2511(1)(c).

370. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class Members, while knowing or having reason to know that the

106

information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Cone Health violated 18 U.S.C. § 2511(1)(d).

371. <u>Unauthorized Purpose</u>. Cone Health intentionally intercepted the contents of Plaintiff's and Class Members' 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, violation of HIPAA and the causes of action described below, among others.

372. The ECPA provides that a "party to the communication" may 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).

373. Cone Health is not a party for purposes to the communication based on its unauthorized duplication and transmission of communications with Plaintiff and the Class. However, even assuming Cone Health is a party, Cone Health's simultaneous, unknown duplication, forwarding, and interception of Plaintiff's and Class Members' Private Information does not qualify for the party exemption.

374. Here, as alleged above, Cone Health violated a provision of HIPAA, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing IIHI to a third party.

375. HIPAA defines IIHI as:

> any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) relates 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 (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

107

376. Plaintiff's and Class Members' information that Cone Health disclosed to third parties qualifies as IIHI, and Cone Health violated Plaintiff's expectations of privacy, and constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6). Cone Health intentionally used the wire or electronic communications to intercept Plaintiff's Private Information in violation of the law.

377. Cone Health's conduct violated 42 U.S.C. § 1320d-6 in that it: Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and disclosed individually identifiable health information to Facebook and/or Google without patient authorization.

378. 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.

379. Cone Health's conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Cone Health's use of the Facebook source code was for Cone Health's commercial advantage to increase revenue from existing patients and gain new patients.

380. Cone Health's acquisition of patient communications that were used and disclosed to Facebook and Google was also 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. Negligence;

    b. Breach of express contract;

    c. Breach of implied contract and

    d. Breach of fiduciary duty.

108

381.     Cone Health is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiff's and Class Members' communications about their Private Information on the Web Properties, because it used its participation in these communications to improperly share Plaintiff's and Class Members' Private Information with Facebook and third-parties that did not participate in these communications, that Plaintiff and Class Members did not know was receiving their information, and that Plaintiff and Class Members did not consent to receive this information.

382.     Here, as alleged above, Cone Health violated a provision of HIPAA, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing individually identifiable health information to a third party.

383.     As such, Cone Health cannot viably claim any exception to ECPA liability.

384.     Plaintiff and Class Members have suffered damages as a direct and proximate result of Cone Health's invasion of privacy in that:

   a. Learning that Cone Health has intruded upon, intercepted, transmitted, shared, and used their PII and PHI (including information about their medical symptoms, conditions, and concerns, medical appointments, healthcare providers and locations, medications and treatments, and health insurance and medical bills) for commercial purposes has caused Plaintiff and the Class Members to suffer emotional distress;

   b. Cone Health 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. Cone Health received substantial, quantifiable value from its use of Plaintiff's and the Class Members' PII and PHI, such as understanding how people use their Web Properties and determining what ads people see on the Web Properties, without providing any value or benefit to Plaintiff or the Class Members;

   d. Cone Health 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 patient information and

109

e. The diminution in value of Plaintiff's and Class Members' PII and PHI and the loss of privacy due to Cone Health making sensitive and confidential information, such as patient status, medical treatment, and appointments that Plaintiff and Class Members intended to remain private no longer private.

385. Cone Health intentionally used the wire or electronic communications to increase revenue. Cone Health specifically used the Meta Pixel and Google tracking code to track and utilize Plaintiff's and Class Members' Private Information for financial gain.

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

387. Plaintiff and Class Members did not authorize Cone Health to acquire the content of their communications for purposes of invading their privacy via the Meta Pixel or Google tracking code.

388. Any purported consent that Cone Health received from Plaintiff and Class Members was not valid.

389. Consumers have the right to rely upon the promises that companies make to them. Cone Health accomplished the tracking and retargeting through deceit and disregard, such that an actionable claim may be made, in that it was accomplished through source code that caused third-party Pixels, tracking codes and cookies (including but not limited to the fbp, ga and gid cookies) and other tracking technologies to be deposited on Plaintiff's and Class members' computing devices as "first-party" cookies that are not blocked.

390. Cone Health's scheme or artifice to defraud in this action consists of:

a. the false and misleading statements and omissions in its privacy policy set forth above, including the statements and omissions recited in the claims below; and

b. the placement of the 'fbp' cookie on patient computing devices disguised as a first-party cookie on Cone Health's Website rather than a third-party cookie from Facebook.

110

391.    Cone Health acted with the intent to defraud in that it willfully invaded and took Plaintiff's and Class Members' property:

a.   property rights to the confidentiality of Private Information and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes; and

b.   property rights to determine who has access to their computing devices.

392.    In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of Cone Health's Web Properties, Cone Health'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.

393.    As a result of Cone Health'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 TWO

### BREACH OF EXPRESS CONTRACT
*(On behalf of Plaintiff & the Nationwide Class)*

394.    Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

111

395. Plaintiff and Class Members allege they entered into valid and enforceable express contracts or were third-party beneficiaries of valid and enforceable express contracts, with Cone Health for the provision of medical and health care services.

396. Specifically, Plaintiff and Class Members entered into a valid and enforceable express contract with Cone Health when Plaintiff first received medical care from Cone Health.

397. The valid and enforceable express contracts to provide medical and health care services that Plaintiff and Class Members entered into with Cone Health include Cone Health's promise to protect nonpublic, Private Information given to Cone Health or that Cone Health gather on its own from disclosure.

398. Under these express contracts, Cone Health and/or their affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b) protect Plaintiff and the Class Members' PII/PHI: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

399. Both the provision of medical services and the protection of Plaintiff and Class Members' Private Information were material aspects of these express contracts.

400. The express contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiff and Class Members' Private Information—are formed and embodied in multiple documents, including (among other documents) Cone Health's Privacy Notice.

401. At all relevant times, Cone Health expressly represented in its Privacy Notice, among other things: (i) that "We are committed to protecting health information about you. We are required by law to make sure that health information that identifies you is kept private, make

112

available to you this notice of our legal duties and privacy practices at Cone Health . . . with respect to health information about you, and follow the terms of the notice that is currently in effect"; and (ii) that "All other information that is shared in a way not addressed in this notice, including uses or disclosures for marketing purposes, or disclosures of your information in exchange for some form of payment, will be made only after you give your written permission or as required by law."[98]

402. Cone Health's express representations, including, but not limited to, express representations found in its Privacy Notice, formed and embodied an express contractual obligation requiring Cone Health to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

403. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security.

404. Plaintiff and Class Members would not have entered into these contracts with Cone Health and/or its affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

405. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Cone Health and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and the protection of their Private Information.

---

[98] https://www.conehealth.com/patients-visitors/privacy/ (last visited June 18, 2024)

406.     Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

407.     Cone Health materially breached its contractual obligation to protect the nonpublic Private Information Cone Health gathered when it disclosed that Private Information to Meta through the Meta Collection Tools, including the Meta Pixel, and to Google through Google Analytics and related technologies embedded on the Web Properties.

408.     Cone Health materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Cone Health did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by Cone Health's sharing of that Private Information with Google and Meta through the Google and Meta Collection Tools on the Web Properties.

409.     The mass and systematic disclosure of Plaintiff's and Class Members' Private Information to third parties, including Meta and Google, was a reasonably foreseeable consequence of Cone Health's actions in breach of these contracts.

410.     As a result of Cone Health's failure to fulfill the data privacy protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts.

411.     Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data privacy protection they paid for and the healthcare they received.

412.     Had Cone Health disclosed that its data privacy was inadequate or that it did not adhere to industry-standard privacy measures, neither the Plaintiffs, the Class Members, nor any

114

reasonable person would have purchased healthcare from Cone Health and/or its affiliated healthcare providers.

413. As a direct and proximate result of the disclosure of Plaintiff's and Class Members' Private Information to Meta and Google, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information, the loss of control and diminution in value of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Cone Health.

414. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the disclosure of Plaintiff's and Class Members' Private Information to Meta and Google.

## COUNT THREE
## BREACH OF IMPLIED DUTY OF GOOD FAITH AND FAIR DEALING
### (On behalf of Plaintiff & the Nationwide Class)

415. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

416. Plaintiff and Class Members allege they entered into valid and enforceable express contracts or were third-party beneficiaries of valid and enforceable express contracts, with Cone Health for the provision of medical and health care services.

417. Specifically, Plaintiff and Class Members entered into a valid and enforceable express contract with Cone Health when Plaintiff first received medical care from Cone Health.

418. The valid and enforceable express contracts to provide medical and health care services that Plaintiff and Class Members entered into with Cone Health include Cone Health's

115

implied duty of good faith and fair dealing, particularly due to Cone Health's special relationship with Plaintiff as her healthcare provider.

419. Under these express contracts, Cone Health and/or their affiliated healthcare providers, promised and were obligated to provide healthcare to Plaintiff and Class Members. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

420. In service of their implied duty of good faith and fair dealing when executing the contract, Cone Health were bound to not voluntarily divulge Plaintiff's and Class Members' sensitive, non-public Private Information to third parties for monetary gain without Plaintiff's and Class Members' consent to such disclosures.

421. The express contracts for the provision of medical services are formed and embodied in multiple documents.

422. As evidence of Cone Health's knowledge of its obligations to perform the contracts in accordance with its implied duty of good faith and fair dealing and Plaintiff's expectations of Cone Health to do the same, at all relevant times, Cone Health expressly represented in its Privacy Notice, among other things: (i) that "We are committed to protecting health information about you. We are required by law to make sure that health information that identifies you is kept private, make available to you this notice of our legal duties and privacy practices at Cone Health . . . with respect to health information about you, and follow the terms of the notice that is currently in effect"; and (ii) that "All other information that is shared in a way not addressed in this notice, including uses or disclosures for marketing purposes, or disclosures of your information in

116

exchange for some form of payment, will be made only after you give your written permission or as required by law."[99]

423. Cone Health's express representations, including, but not limited to, express representations found in its Privacy Notice, evidence Cone Health's knowledge of the specific manifestations of its duty to perform the contracts in accordance with its implied duty of good faith and fair dealing, which required Cone Health to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

424. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security.

425. Plaintiff and Class Members would not have entered into these contracts with Cone Health and/or its affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

426. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Cone Health and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and, through Cone Health's implied duty of good faith and fair dealing, the protection of their Private Information.

427. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

---

[99] https://www.conehealth.com/patients-visitors/privacy/ (last visited June 18, 2024)

117

428. Cone Health did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by Cone Health's sharing of that Private Information with Google and Meta through the Google and Meta Collection Tools on the Web Properties.

429. Cone Health breached its implied duty of good faith and fair dealing to protect the nonpublic Private Information Cone Health gathered when it disclosed that Private Information to Google and Meta through the Google and Meta Collection Tools on the Web Properties.

430. The mass and systematic disclosure of Plaintiff's and Class Members' Private Information to third parties, including Meta and Google, was a reasonably foreseeable consequence of Cone Health's actions in breach of its implied duty of good faith and fair dealing.

431. As a result of Cone Health's failure to fulfill the data privacy protections inherent in the special relationship with Plaintiff and the Class Members, and resulting breach of their implied duty of good faith and fair dealing, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts.

432. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data privacy protection they paid for and the healthcare they received.

433. Had Cone Health disclosed that its data privacy was inadequate or that they did not adhere to industry-standard privacy measures, neither the Plaintiffs, the Class Members, nor any reasonable person would have purchased healthcare from Cone Health and/or its affiliated healthcare providers.

434. As a direct and proximate result of the disclosure of Plaintiff's and Class Members' Private Information to Meta, Plaintiff and Class Members have been harmed and have suffered,

118

and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information, the loss of control and diminution in value of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Cone Health.

435.    Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the disclosure of Plaintiff's and Class Members' Private Information to Meta and Google.

## COUNT FOUR

### BREACH OF IMPLIED CONTRACT
### *(On behalf of Plaintiff & the Nationwide Class)*

436.    Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

437.    Plaintiff and Class Members allege they entered into valid and enforceable implied contracts or were third-party beneficiaries of valid and enforceable implied contracts, with Cone Health for the provision of medical and health care services.

438.    Specifically, Plaintiff and Class Members entered into a valid and enforceable contract with Cone Health when Plaintiff first received medical care from Cone Health.

439.    The valid and enforceable contracts to provide medical and health care services that Plaintiff and Class Members entered into with Cone Health include Cone Health's promise to protect nonpublic, Private Information given to Cone Health or that Cone Health gathers on its own from disclosure.

440.    Under these contracts, Cone Health and/or its affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b)

119

protect Plaintiff and the Class Members' PII/PHI: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

441. Both the provision of medical services and the protection of Plaintiff and Class Members' Private Information were material aspects of these contracts.

442. The contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiff and Class Members' Private Information—are formed and embodied in multiple documents, including (among other documents) Cone Health's Privacy Notice.

443. At all relevant times, Cone Health expressly represented in its Privacy Notice, among other things: (i) that "We are committed to protecting health information about you. We are required by law to make sure that health information that identifies you is kept private, make available to you this notice of our legal duties and privacy practices at Cone Health . . . with respect to health information about you, and follow the terms of the notice that is currently in effect"; and (ii) that "All other information that is shared in a way not addressed in this notice, including uses or disclosures for marketing purposes, or disclosures of your information in exchange for some form of payment, will be made only after you give your written permission or as required by law."[100]

444. Cone Health's express representations, including, but not limited to, express representations found in its Privacy Notice, formed and embodied an express contractual obligation requiring Cone Health to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

---

[100] https://www.conehealth.com/patients-visitors/privacy/ (last visited June 18, 2024)

445.     Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiff and Class Members would not have entered into these contracts with Cone Health and/or its affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

446.     A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Cone Health and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and the protection of their Private Information.

447.     Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

448.     Cone Health materially breached its contractual obligation to protect the nonpublic Private Information Cone Health gathered when it disclosed that Private Information to Google and Meta through the Google and Meta Collection Tools on the Web Properties.

449.     Cone Health materially breached the terms of these contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Cone Health did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by Cone Health's sharing of that Private Information with Google and Meta through the Google and Meta Collection Tools on the Web Properties.

121

450. The mass and systematic disclosure of Plaintiff's and Class Members' Private Information to third parties, including Meta and Google, was a reasonably foreseeable consequence of Cone Health's actions in breach of these contracts.

451. As a result of Cone Health's failure to fulfill the data privacy protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data privacy protection they paid for and the healthcare they received.

452. Had Cone Health disclosed that its data privacy was inadequate or that it did not adhere to industry-standard privacy measures, neither the Plaintiffs, the Class Members, nor any reasonable person would have purchased healthcare from Cone Health and/or its affiliated healthcare providers.

453. As a direct and proximate result of the disclosure of Plaintiff's and Class Members' Private Information to Meta and Google, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information, the loss of control and diminution in value of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Cone Health.

454. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the disclosure of Plaintiff's and Class Members' Private Information to Meta and Google.

122

**COUNT FIVE**

**NEGLIGENCE**
*(On behalf of Plaintiff & the Nationwide Class)*

455.    Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

456.    Cone Health required Plaintiff and Class Members to submit non-public personal information in order to obtain healthcare services.

457.    Upon accepting, storing, and controlling the Private Information of Plaintiff and the Class in their computer systems, Cone Health owed, and continues to owe, a duty to Plaintiff and the Class to exercise reasonable care to secure, safeguard and protect their highly sensitive Private Information from disclosure to third parties.

458.    Cone Health's duty of care to use reasonable measures to secure and safeguard Plaintiff's and Class Members' Private Information arose due, in part, to the special relationship that existed between Cone Health and its patients, which is recognized by statute, regulations, and the common law.

459.    In addition, Cone Health had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

460.    Cone Health's duty to use reasonable security measures under HIPAA required Cone Health to "reasonably protect" confidential data from "any intentional or unintentional use

123

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).

461. 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.

462. In addition, Cone Health had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission 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.

463. Cone Health's duty to use reasonable care in protecting confidential data arose also because Cone Health is bound by industry standards to protect confidential Private Information.

464. Cone Health breached this duty by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

465. It was reasonably foreseeable that Cone Health's failures to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' Private Information through its use of the Google and Meta Collection Tools and other tracking technologies would result in unauthorized third parties, such as Facebook and Google, gaining access to such Private Information for no lawful purpose.

466. Cone Health's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their Private Information.

467. Cone Health's misconduct included the failure to (1) secure Plaintiff's and Class Members' Private Information; (2) comply with industry standard data security practices; (3) implement adequate website and event monitoring; (4) implement the systems, policies, and

124

procedures necessary to prevent unauthorized disclosures resulting from the use of the Google and Meta Collection Tools and other tracking technologies; and (5) prevent unauthorized access to Plaintiff's and Class Members' Private Information by sharing that information with Meta, Google and other third parties. Cone Health's failures and breaches of these duties constituted negligence.

468.    As a direct result of Cone Health's breaches of its duty of confidentiality and privacy and the disclosure of Plaintiff's and Class members' Private Information, Plaintiff and the Class have suffered damages that include, without limitation, loss of the benefit of the bargain, increased infiltrations into their privacy through spam and targeted advertising they did not ask for, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

469.    Cone Health's wrongful actions and/or inactions and the resulting unauthorized disclosure of Plaintiff's and Class members' Private Information constituted (and continue to constitute) negligence at common law.

470.    Plaintiff and Class Members are entitled to compensatory, nominal, and/or punitive damages, and Plaintiff and Class Members are entitled to recover those damages in an amount to be determined at trial.

471.    Cone Health'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 Cone Health to (i) strengthen its data security systems and monitoring procedures; (ii) cease sharing Plaintiff's and Class Members' Private Information with Meta, Google and other third parties without Plaintiff's and Class Members' express consent; and (iii) submit to future annual audits of its security systems and monitoring procedures.

125

## COUNT SIX

## BREACH OF FIDUCIARY DUTY
### (*On Behalf of Plaintiff & the Nationwide Class*)

472.    Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

473.    In light of the special physician-patient relationship between Cone Health and Plaintiff and Class Members, which was created for the purpose of Cone Health providing healthcare to Plaintiff and Class Members, Cone Health became guardian of Plaintiff's and Class Members' Private Information. Cone Health became a fiduciary by their 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) Cone Health did and do store.

474.    Cone Health has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant' relationship with its patients and former patients, in particular, to keep secure their Private Information.

475.    Cone Health breached its fiduciary duty to Plaintiff and Class Members by disclosing their Private Information to unauthorized third parties, including Meta and Google, and separately, by failing to notify Plaintiff and Class Members of this fact.

476.    As a direct and proximate result of Cone Health's breaches of its fiduciary duty, 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.

126

**UNJUST ENRICHMENT**
*(On behalf of Plaintiff & Nationwide Class)*

477. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein, except for the paragraphs specifically regarding breach of contract.

478. Plaintiff plead this claim in the alternative to their breach of contract claim.

479. Plaintiff and Class Members personally and directly conferred a benefit on Cone Health by paying Cone Health for health care services, which included Cone Health's obligations to protect Plaintiff's and Class Members' Private Information. Cone Health was aware of Plaintiff's privacy expectations, and in fact, promised to maintain Plaintiff's Private Information confidential and not to disclose to third parties. Cone Health received payments for medical services from Plaintiff and Class Members.

480. Plaintiff and Class Members also conferred a benefit on Cone Health in the form of valuable sensitive medical information that Cone Health collected from Plaintiff and Class Members under the guise of keeping this information private.

481. Cone Health collected, used, and disclosed this information for its own gain, including for advertisement, market research, sale, or trade for valuable benefits from Facebook, Google and other third parties.

482. Cone Health had knowledge that Plaintiff and Class Members had conferred this benefit on Cone Health by interacting with the Web Properties, and Cone Health intentionally installed the Google and Meta Collection Tools on the Web Properties to capture and monetize this benefit conferred by Plaintiff and Class Members.

127

483. Plaintiff and Class Members would not have used Cone Health's Web Properties had they known that Cone Health would collect, use, and disclose this information to Facebook, Google, and other third parties.

484. The services that Plaintiff and Class Members ultimately received in exchange for the monies paid to Cone Health were worth quantifiably less than the services that Cone Health promised to provide, which included Cone Health's promise that any patient communications with Cone Health would be treated as confidential and would never be disclosed to third parties for marketing purposes without the express consent of patients.

485. The medical services that Cone Health offers are available from many other health care systems that do protect the confidentiality of patient communications. Had Cone Health disclosed that it would allow third parties to secretly collect Plaintiff's and Class Members' Private Health Information without consent, neither Plaintiff, the Class Members, nor any reasonable person would have purchased healthcare from Cone Health and/or its affiliated healthcare providers.

486. By virtue of the unlawful, unfair and deceptive conduct alleged herein, Cone Health knowingly realized hundreds of millions of dollars in revenue from the use of the Private Information of Plaintiff and Classes Members by way of targeted advertising related to Users' respective medical conditions and treatments sought.

487. This Private Information, the value of the Private Information, and/or the attendant revenue, were monetary benefits conferred upon Cone Health by Plaintiff and Class Members.

488. As a result of Cone Health's conduct, Plaintiff and Class Members suffered actual damages in the loss of value of their Private Information and the lost profits from the use of their Private Information.

128

489. It would be inequitable and unjust to permit Cone Health to retain the enormous economic benefits (financial and otherwise) it obtained from and/or at the expense of Plaintiff and Class Members.

490. Cone Health will be unjustly enriched if it is permitted to retain the economic benefits conferred upon it by Plaintiff and Class Members through Cone Health's obtaining the Private Information and the value thereof, and financially benefitting from the unlawful, unauthorized and impermissible use of the Private Information of Plaintiff and Class Members.

491. Plaintiff and Class Members are therefore entitled to recover the amounts realized by Cone Health at the expense of Plaintiff and Class Members.

492. Plaintiff and the Class Members have no adequate remedy at law and are therefore entitled to restitution, disgorgement, and/or the imposition of a constructive trust to recover the amount of Cone Health's ill-gotten gains, and/or other sums as may be just and equitable.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiff, on behalf of herself and the Proposed Class defined herein, respectfully requests this Honorable Court to provide the following relief:

A. That this Action be maintained as a Class Action, that Plaintiff be named as Class Representative of the Class, that the undersigned be named as Lead Class Counsel of the Class, and that notice of this Action be given to Class Members;

B. That the Court enter an order:

  1. Preventing Cone Health from sharing Plaintiff's and Class Members' Private Information among other third parties;

  2. Requiring Cone Health to alert and/or otherwise notify all Users of the Web Properties of what information is being collected, used, and shared;

  3. Requiring Cone Health to provide clear information regarding its practices concerning data collection from the Users/patients of Cone Health's Web Properties, as well as uses of such data;

129

4. Requiring Cone Health to establish protocols intended to remove all personal information which has been leaked to Facebook, Google and/or other third parties, and request Facebook/Google/third parties to remove such information;

5. Requiring Cone Health to provide an opt out procedure for individuals who do not wish for their information to be tracked while interacting with Cone Health's Web Properties;

6. Mandating the proper notice be sent to all affected individuals, and posted publicly;

7. Requiring Cone Health to delete, destroy, and purge the Private Information of Users unless Cone Health can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Users;

8. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

C. That the Court award Plaintiff and the Class Members damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

D. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against Cone Health to which Plaintiff and the Class are entitled, including but not limited to restitution and an Order requiring Cone Health to cooperate and financially support civil and/or criminal asset recovery efforts;

E. Plaintiff and the Class be awarded with pre- and post-judgment interest (including pursuant to statutory rates of interest set under State law);

F. Plaintiff and the Class be awarded with the reasonable attorneys' fees and costs of suit incurred by their attorneys;

G. Plaintiff and the Class be awarded with treble and/or punitive damages insofar as they are allowed by applicable laws; and

H. Any and all other such relief as the Court may deem just and proper under the circumstances.

## JURY TRIAL DEMANDED

Plaintiff demands a jury trial on all triable issues.

DATED: July 8, 2024                    Respectfully Submitted,

                                   By:  _/s/ David M. Wilkerson_____
130

David M. Wilkerson, N.C. Bar No. 35742
Attorney for Plaintiff
The Van Winkle Law Firm
11 N. Market Street
Asheville, NC 28801
(828) 258-2991
dwilkerson@vwlawfirm.com

**PEIFFER WOLF CARR
KANE CONWAY & WISE, LLP**

Brandon M. Wise
IL Bar # 6319580*
One US Bank Plaza, Suite 1950
St. Louis, MO 63101
Ph: (314) 833-4825
bwise@peifferwolf.com

Andrew R. Tate
GA Bar # 518068*
235 Peachtree St. NE, Suite 400
Atlanta, GA 30303
Ph: 404-282-4806
atate@peifferwolf.com

**ALMEIDA LAW GROUP LLC**

David S. Almeida
NY Bar # 3056520*
Britany Kabakov
IL Bar # 6336126*
849 W. Webster Avenue
Chicago, Illinois 60614
Ph: (312) 576-3024
david@almeidalawgroup.com
britany@almeidalawgroup.com

*pro hac vice to be sought*

*Counsel for Plaintiff & the Proposed Class*

131