

**IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF INDIANA  
INDIANAPOLIS DIVISION**

BRIAN ALEXANDER-FETTERMAN,  
ERIC MARKSON, JENAY  
REYNOLDS-SIBBACH, AARON  
ROSEN, KEVIN SMITH, and NANCY  
WINCHESTER, individually and on  
behalf of all others similarly situated,

*Plaintiffs,*

v.

ANTHEM INSURANCE COMPANIES,  
INC., and ELEVANCE HEALTH, INC.  
f/k/a ANTHEM, INC.,

*Defendants.*

CLASS ACTION

Civil Action No. 1:25-cv-2282-MPB-MG

DEMAND FOR JURY TRIAL

**AMENDED CLASS ACTION COMPLAINT**

1. Plaintiffs Brian Alexander-Fetterman, Eric Markson, Jenay Reynolds-Sibbach, Aaron Rosen, Kevin Smith, and Nancy Winchester (“Plaintiffs”), individually and on behalf of all others similarly situated, bring this class action lawsuit against Defendants Anthem Insurance Companies, Inc. (“Anthem”) and Elevance Health, Inc. f/k/a Anthem, Inc. (“Elevance”) for violations of the Federal Wiretap Act, 18 U.S.C. § 2510 et seq. (“FWA”), breach of fiduciary duty, intrusion upon seclusion, and unjust enrichment under Indiana common law. Plaintiffs allege the following facts based upon personal knowledge, investigation by counsel, and information and belief.

2. Elevance (along with its public-facing subsidiary, Anthem) wiretapped its insureds in a brazen and invasive betrayal of trust. Defendants harvested highly

sensitive health-related information from their insureds using hidden tracking tools, and secretly disseminated this private health-related information to third parties. Plaintiffs were not notified of Defendants' hidden tracking and harvesting of their private information, which began as soon as Plaintiffs loaded Defendants' website. Nor were Plaintiffs provided any opportunity to limit or consent to Defendants' tracking and harvesting of their personal health information.

3. Defendants' public-facing representations about their privacy practices were inadequate and affirmatively misleading, including because Defendants stated that no disclosure of Plaintiffs' private data would occur absent Plaintiffs' express written authorization. Yet, even on webpages describing Defendants' purported privacy practices, Defendants surreptitiously tracked and disseminated Plaintiffs' private health-related information, including to third parties Medallia, Inc. ("Medallia"), Quantum Metric, Inc. ("Quantum Metric"), and Adobe Inc. ("Adobe").

4. Even within Defendants' purportedly secure patient portals – where insureds access claims, prescriptions, and sensitive medical tools designed to help identify ailments and health issues – Defendants' surreptitious tracking of Plaintiffs' private health-related information was constant and pervasive, and the highly sensitive health-related data of Plaintiffs and other insureds were immediately transmitted, in real time, to third-party servers operated by Quantum Metric and Adobe without any form of consent.

5. Plaintiffs seek damages and injunctive relief to redress Defendants' unlawful interception and misuse of their private health-related information.

## **NATURE OF THE CASE**

### **A. Defendants' Interception of Website and Portal Communications**

6. This action challenges Defendants' practice of surreptitiously intercepting and misusing personal, and highly sensitive, health-related information from Defendants' www.anthem.com website, including the password-protected patient portals through which insureds log in to review claims, manage prescriptions, and complete health assessments (together with subpages, Defendants' "Website").

7. Defendants have violated, and continue to violate, the FWA and Indiana common law by wiretapping the private electronic health-related communications of Plaintiffs and other users of Defendants' Website.

8. Defendants' violations occur as follows: Entirely unbeknownst to site and portal users, third-party vendors, including Quantum Metric, Adobe, and Medallia (collectively, "Third-Party Vendors"), have supplied tracking technologies ("Tracking Pixels" and "Session Replay Code," or "Tracking Technologies") to Defendants, which Defendants have embedded in their Website.

9. These tracking technologies load immediately on both public-facing pages of Defendants' Website and within purportedly secure portals for covertly tracking, intercepting, and recording Website users' communications with Defendants, including but not limited to users' keystrokes (i.e., text entered into a search box or information box), web addresses (i.e., "URLs") of individual pages visited, mouse movements, clicks, and/or other electronic communications in real time ("Website Communications").

10. After surreptitiously intercepting and capturing the Website Communications of users of the Website, Defendants and the Third-Party Vendors use these Website Communications for purposes that benefit and enrich themselves.

11. The Third-Party Vendors use the harvested personal health-related information they obtain to create and/or bolster advertising profiles of Website users, to target or retarget advertisements to users, and/or to sell information about Website users to other entities for commercial gain.

12. Defendants use the harvested information to track visits to the Website, allowing Defendants to covertly recreate Website users' entire sessions on Defendants' Website. This includes detailed replays of portal sessions, such as when insureds search for providers, review "My Health" assessments, or access benefits and prescription information.

13. Defendants also use the embedded code that loads immediately on the Website to create a replay of users' behavior on the Website.

14. This collection of Website and portal users' highly sensitive, private data takes place without notice to or consent from users of Defendants' Website.

15. Defendants cause the collection of this highly sensitive, private data by embedding the code of Tracking Technologies, such as Tracking Pixels, in the Website. The embedded code instantly sends private health-related data to the Third-Party Vendors.

16. Defendants thereby permit the Third-Party Vendors to intercept Website users' private health-related information.

17. Defendants benefit financially by obtaining and analyzing data that enables them to add new customers, replacing the need for (and costs associated with) advertising, and surreptitiously finding targets for advertising campaigns.

18. These commercial advantages come at the expense of insureds' privacy and contradict Defendants' online promises to safeguard health-related information and legal duty to do the same.

## **B. Defendants' Legal Duties and Resulting Harms**

19. Defendants' violations have broad-ranging deleterious effects, including because Defendants hold highly sensitive personal, health-related data of their insureds. These data include private medical and health information, as well as related unique personal identifiers, health details, and other data provided by insureds related to or for the purpose of obtaining healthcare.

20. Federal privacy laws require robust privacy protections for these highly sensitive personal, health-related data.

21. Elevance is a covered entity under the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. § 1320d *et seq.*, because it operates health plans.

22. A business associate is an entity that performs activities on behalf of, or provides services to, a covered entity involving the use or disclosure of protected health information ("PHI"). *See* 45 C.F.R. § 160.103.

23. Elevance is a business associate under HIPAA because it performs services involving PHI on behalf of its health plan subsidiaries. These services

include but are not limited to data analysis and reporting, claims administration, member communication or outreach, and other reviews.

24. Anthem is a covered entity under HIPAA because it meets the statutory and regulatory requirements of a health plan. *See* 45 C.F.R. § 160.103.

25. Under HIPAA, a covered entity or business associate must comply with HIPAA privacy and security rules with respect to individually identifiable health information, or PHI. *See* 45 C.F.R. §§ 164.302–316; 164.500–534.

26. Covered entities or business associates are required to implement administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of PHI. 45 C.F.R. § 164.306.

27. Covered entities or business associates are prohibited from using or disclosing PHI except as permitted by law. *See* 45 C.F.R. §§ 164.502(a)(3); 164.504(e).

28. Disclosure of PHI for marketing or analytics purposes – such as to data brokers or advertising networks – is expressly prohibited absent valid, written authorization. *See* 45 C.F.R. § 164.508(a)(3) (“a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing”); *id.* § 164.508(c)(1)(vi).

29. Defendants act as fiduciaries with respect to the sensitive data that they collect and manage on behalf of Plaintiffs.

30. By designing, operating, and maintaining the Website through which Plaintiffs access password-protected health benefit information, Defendants assume

the responsibility and duty to safeguard these data and use them solely for authorized, health-related purposes.

31. This fiduciary duty includes a duty of loyalty and care, requiring Defendants to avoid exploiting Plaintiffs' data for commercial benefit or disclosing data to third parties like the Third-Party Vendors without clear, informed, and express consent.

32. As a result of Defendants' violations and invasions of the privacy rights of their insureds, these insureds, including Plaintiffs, have suffered significant harms, including but not limited to a loss of privacy and control over their private health-related data, greatly increased vulnerability to identity theft and fraud, and the surreptitious use of their confidential financial and health-related information for the benefit of Defendants and others, without any consent.

33. Plaintiffs bring this action individually and on behalf of a nationwide class of all insureds of Defendants whose Website Communications were wiretapped and intercepted via the code embedded in Defendants' Website.

34. Plaintiffs seek all civil remedies provided under the alleged causes of action, including but not limited to compensatory, statutory, treble, and/or punitive damages, and attorneys' fees and costs.

## **PARTIES**

### **A. Plaintiffs**

35. Plaintiff Brian Alexander-Fetterman is a resident of Lakewood in Los Angeles County, California. He has been insured under a health policy of Anthem through his employer, California State University, Long Beach, since 2025. During

the relevant time periods, he regularly used Defendants' Website, including to review medical billing information, search for physicians, review claims, and review explanations of benefits.

36. Plaintiff Eric Markson is a resident of Westerlo in Albany County, New York. He has been insured under a health policy of Anthem through his employer since approximately May 2024. During the relevant time periods, he routinely visited Defendants' Website, including to view his claims and the status of his prior authorizations.

37. Plaintiff Jenay Reynolds-Sibbach is a resident of Atascadero in San Luis Obispo County, California. She was insured under a health policy of Anthem through her employer, California Polytechnic State University, San Luis Obispo, from approximately 2009 to 2024. She routinely used Defendants' Website, including to review her claims and benefits, verify the accuracy of billing statements, submit out-of-network claims, search for physicians, check the status of her deductible, and access her patient portal.

38. Plaintiff Aaron Rosen is a resident of Canal Winchester in Franklin County, Ohio. He has been insured under a health policy of Anthem through his employer for approximately the past 14 years. He has used and continues to use Defendants' Website, including to order medication, access information regarding his claims, search for providers, schedule appointments, and check the status of his deductible.

39. Plaintiff Kevin Smith is a resident of Oakland in Alameda County, California. As a former employee of Anthem, he was insured under an Anthem health policy from approximately 2020 to 2024. During the relevant time periods, he used Defendants' Website regularly, including to search for providers for himself and his children, order medication, schedule appointments, check the status of his deductible, view explanations of benefits, and view claims.

40. Plaintiff Nancy Winchester is a resident of Humble in Harris County, Texas. She has been insured under a health policy of Anthem through her employer for approximately the past two years. During the relevant time periods, she routinely used Defendants' Website, including to search for providers, estimate costs of procedures, and view explanations of benefits.

## **B. Defendants Elevance and Anthem**

41. Elevance is one of the largest health insurance and health service providers in the United States, ranking third by net premiums written, with nearly \$143 billion in 2023 net premiums written.<sup>1</sup> It is a publicly traded corporation incorporated in Indiana and headquartered in Indianapolis, Indiana.

42. Elevance was formerly known as Anthem, Inc., until 2022, when it changed its corporate name.<sup>2</sup>

---

<sup>1</sup> David Pilla, *Health Underwriters Dominate in Best's World's Largest Insurers*, AM BestWire (Jan. 3, 2025), <https://news.ambest.com/newscontent.aspx?refnum=263284&altsrc=23>. [<https://perma.cc/88JF-7HFS>].

<sup>2</sup> Press Release, Elevance Health, *Anthem, Inc. Shareholders Approve Corporate Rebranding to New Name, Elevance Health Inc.*, ELEVANCE HEALTH (May 18, 2022), <https://www.elevancehealth.com/newsroom/anthem-inc-shareholders-approve-corporate-rebranding-new-name> [<https://perma.cc/CNQ2-FGRH>].

43. Elevance operates subsidiaries that provide health insurance services to individuals and employers nationwide.

44. Defendant Anthem is a subsidiary of Elevance that provides health insurance services.

45. Anthem is also incorporated in Indiana and maintains its principal place of business in Indianapolis, Indiana.

46. Despite Elevance's re-naming, Anthem still uses "Anthem" as a brand name for its insurance products and website.

47. Elevance and Anthem jointly oversee the Anthem-branded digital infrastructure used by insureds, including Plaintiffs, to access their health plan information. This infrastructure includes the Website, which Elevance and Anthem operate and control.

48. Defendants' Website includes a portal through which insureds, including Plaintiffs, research and seek advice on highly sensitive health issues, manage health benefits, verify doctors, and access information about their personal healthcare coverage.

49. In 2024, Elevance generated approximately \$175.2 billion in operating revenue, an increase of about 3 percent over 2023.<sup>3</sup>

50. Elevance and Anthem are both "person[s]" as defined in the FWA. 18 U.S.C. § 2510(6).

---

<sup>3</sup> *Health Reports Results for Fourth Quarter and Full Year 2024; Sets Full Year 2025 Outlook*, ELEVANCE HEALTH (Jan. 23, 2025), <https://www.elevancehealth.com/newsroom/elv-quarterly-earnings-q4-2024> [<https://perma.cc/357A-N3P8>].

**C. Elevance's Principal Liability for the Acts of its Agent, Anthem**

51. Elevance's disclosures<sup>4</sup> with the U.S. Securities and Exchange Commission ("SEC") show that it delivers healthcare through a network of affiliated health plans operating under the Elevance umbrella.

52. Elevance's disclosures admit that Elevance sets policies and manages operations across its subsidiaries, including Anthem.

53. Elevance's disclosures further note that Anthem is a subsidiary in which Elevance holds "50% and above" ownership.<sup>5</sup>

54. Under Indiana law, an agency relationship exists when one party acts for another and is subject to that party's control.

55. At all relevant times, Elevance directed and controlled the operations of Anthem, particularly Anthem's work on the Website that served as the online platform for engagement with Anthem's insureds, including Plaintiffs.

56. Anthem acts with actual authority from Elevance to operate the Website, which includes authority over everything from how users navigate the Website, what information is available, how data are collected, and what Third-Party Vendor code is embedded on the Website.

57. Anthem advances Elevance's goals, including but not limited to gathering valuable data about Plaintiffs' interactions with the Website, which

---

<sup>4</sup> See Elevance Health Inc., *Annual Report* (Form 10-K) (filed Mar. 1, 2025), at 76, [https://s202.q4cdn.com/665319960/files/doc\\_financials/2025/ar/Elevance-Health-2024-10K-color.pdf](https://s202.q4cdn.com/665319960/files/doc_financials/2025/ar/Elevance-Health-2024-10K-color.pdf) [<https://perma.cc/LQA2-PY4V>].

<sup>5</sup> Elevance Health, Inc., *Exhibit 21 – List of Subsidiaries* (Form 10-K) (filed Mar. 1, 2025), <https://www.sec.gov/Archives/edgar/data/1156039/000115603925000010/exhibit21-20241231forform1.htm> [<https://perma.cc/4S6W-SF9H>].

benefits Elevance by providing Elevance with data in a competitive insurance marketplace and additional revenue.

58. Elevance retains the exclusive right to control the Website, including the right to make decisions about what data get collected, how these data are used, and how Tracking Technologies are implemented.

59. As such, Elevance is legally responsible for Anthem's conduct under Indiana agency law, including all of the conduct at issue in this action, and is directly responsible itself, independent of its role as the principal, for these acts.

### **JURISDICTION**

60. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action in which the aggregate claims of all members of the proposed class are in excess of \$5,000,000.00, exclusive of interest and costs; there are 100 or more members of the proposed class; and at least one member of the proposed class, including Plaintiffs, is a citizen of a state different than Defendants.

61. Defendants' Website includes a "Terms of Use" section that provides:

These Terms of Use ("Terms") apply to those mobile applications and websites that we operate (each an "Application") and that contain a link to these Terms. By using our Applications you are agreeing to these Terms. Please read them carefully.<sup>6</sup>

62. These terms of use form an agreement between Website users, including Plaintiffs, and Defendants.

---

<sup>6</sup> *Anthem Terms Of Use*, ANTHEM HEALTHCARE, <https://www.anthem.com/terms-of-use> (last updated November 1, 2016) [<https://perma.cc/4SUY-MFL6>].

63. Plaintiffs used the Website and therefore accepted these terms of use and entered into a direct agreement with Defendants.

64. Defendants' terms of use do not contain any disclosures regarding Defendants' use of Tracking Technologies, and do not incorporate or even reference any of Defendants' privacy policies. Defendants' terms of use do not mention user data at all.

65. Defendants have consented to personal jurisdiction in the Southern District of Indiana as part of their terms of use. As those terms provide:

These Terms shall be governed and construed in accordance with the laws of the State of Indiana without regard to the choice of law provisions of any jurisdiction. We may without notice to you assign our rights and duties under these Terms to any party at any time. Failure to enforce or insist on strict performance of any provision of these Terms shall not be construed as a waiver of any provision or right. *You agree that any legal action or proceeding between us and you in any way related to these Terms shall be brought exclusively in a court of a competent jurisdiction sitting in Indianapolis, Indiana.*<sup>7</sup>

66. By using Defendants' Website and services, insureds (including Plaintiffs) agreed to this clause, thereby submitting to jurisdiction in this District for any legal disputes.

67. This is commonly known as a "forum selection clause."

68. The forum selection clause designating this District as the venue for its legal disputes is not unreasonable because both Defendants expect to resolve disputes in this District and have a significant presence in this District in that both Anthem and Elevance have their corporate headquarters in this District.

---

<sup>7</sup> *Id.* (emphasis added).

69. Jurisdiction in this District is neither arbitrary nor inconvenient for Defendants, as it is where they both conduct substantial business.

70. Elevance has consented to jurisdiction in this Court because it is held to the agreements made by its agent, Anthem, while acting on Elevance's behalf.

### **THE FEDERAL WIRETAP ACT**

71. Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968, known as the Federal Wiretap Act, to protect the privacy of wire, oral, and electronic communications from unauthorized interception, disclosure, and use. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 801-804, 82 Stat. 197, 211-225.

72. In 1986, Congress passed a law called the Electronic Communications Privacy Act ("ECPA") to amend the FWA in order protect the privacy of electronic communications. Pub. L. No. 99-508, 100 Stat. 1848.

73. The ECPA was enacted to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." S. Rep. No. 99-541, at 1 (1986), as reprinted in 1986 U.S.C.C.A.N. 3555, 3555.

74. Title I of the ECPA amended the FWA to expand its coverage beyond wire and oral communication and "address[ ] the interception of . . . electronic communications." S. Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3557.

75. The “paramount objective of the [ECPA, which amended the Wiretap Act] is to protect effectively the privacy of communications.”<sup>8</sup>

76. The FWA defines “person” to include “any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.” 18 U.S.C. § 2510(6).

77. The FWA prohibits any “person” from (1) intentionally intercepting, endeavoring to intercept, or procuring another person to intercept or endeavor to intercept any wire, oral, or electronic communication, (2) intentionally disclosing, or endeavoring to disclose, the contents of any such communication knowing or having reason to know it was unlawfully intercepted, or (3) intentionally using, or endeavoring to use, the contents of any such communication knowing or having reason to know it was unlawfully intercepted. 18 U.S.C. § 2511(1).

78. The FWA, as amended by the ECPA, defines “electronic communication” as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system.” 18 U.S.C. § 2510(12).

79. The term “contents,” with respect to communications, includes “any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8).

---

<sup>8</sup> *Joffe v. Google*, 746 F.3d 920, 931 (9th Cir. 2013) (quoting *In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9, 18 (1st Cir. 2003)).

80. The FWA provides a civil cause of action to “[a]ny person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter” against the person or entity who engaged in such conduct. 18 U.S.C. § 2520(a).

81. The FWA permits recovery of preliminary and permanent injunctive relief, the greater of actual damages or statutory damages calculated at \$100 per day or \$10,000 per violation, punitive damages, and attorneys’ fees and costs. 18 U.S.C. § 2520(b)–(c).

82. Although the FWA includes an exception permitting interception with the consent of “one of the parties to the communication,” this exception does not apply where the interception is done “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” (also commonly known as the “crime-tort exception”). 18 U.S.C. § 2511(2)(d).

### **FACTUAL ALLEGATIONS**

#### **I. How Websites Can Use Code to Harvest Users’ Private Information**

##### **A. Websites Can Be Used to Harvest Personal Data from Users**

83. Web browsers are software applications that allow users to navigate the Internet and view and exchange electronic information and communications.

84. Each “device” (such as a computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google’s Chrome browser, Mozilla’s Firefox browser, Apple’s Safari browser, and Microsoft’s Edge browser).

85. Websites are hosted on servers, which are computers that store the site's data and facilitate the exchange of information between the website and the users' browsers.

86. An HTTP request is a message sent from a web browser to a website's server to ask for information, such as loading a webpage or submitting a query.

87. An HTTP response is the message that a website's server sends in response to an HTTP request to the browser. It includes the requested information.

88. Web interactions involve HTTP requests and HTTP responses, with each browsing session typically involving thousands of these exchanges.

89. When a user visits a website, the website sends a small amount of data, known as a "cookie," to be stored on the user's browser.

90. Cookies are then stored locally on the user's browser and included with future requests to the same server.

91. Cookies are used to "remember" users between sessions, including how users interact with the website.

92. When users log into a website and it "remembers" them, it is often because of a cookie.

93. Because of the data and privacy concerns associated with cookies, many legal jurisdictions regulate their use. For example, California's Consumer Privacy Act requires businesses to disclose the use of cookies, and the European Union's General Data Protection Regulation mandates user consent before cookies are placed on devices.

94. When a user visits a website, the browser sends an HTTP request to the server, requesting specific information – for example, the “select a type of coverage” menu on Defendants’ Website.

95. The server responds with an HTTP response, which includes the requested data in the form of “markup.”

96. This markup is the underlying structure for what the user sees on the webpage, such as text, images, and interactive elements.

97. Websites are built using this markup and “source code,” which provides instructions to the browser, dictating how the page behaves when it loads or when a particular action occurs.

98. Source code may be written to include instructions to send data to third parties via background HTTP requests.

99. Users may be unaware that data are being sent to third parties.

100. These background requests can be designed to function like a digital wiretap, capturing and transmitting communications, and facilitating the covert harvesting of consumer data.

101. Source code may also be written to send user data outward.

102. This source code can send information – like searches or messages – from the user’s browser to the website’s server.

103. The requests contained in source code can secretly send user data to third parties, because the requests send data via the HTTP request and not in a

visible place like the browser's address bar, so users are generally unaware that any data transmissions are even occurring.

104. When source code is written to send these data requests to third-party tracking domains and servers (especially in real time), the third parties receive user data, including data that users may not have intended to disclose.

## **II. Tracking Pixels and Session Replay Code Can Be Used to Extract Individuals' Private Information**

105. Tracking Pixels include a broad range of HTML and JavaScript code embedded in websites and emails.<sup>9</sup>

106. Tracking Pixels are hidden from sight.

107. Tracking Pixels trigger a network traffic request to the tracking entity's remote server.

108. By triggering this network traffic request, Tracking Pixels can track, collect, and send to third parties various private and/or personal data, such as how a user interacts with the website or information typed into text fields.<sup>10</sup>

109. Because Tracking Pixels embedded into websites such as Defendants' Website operate silently in the background, users often do not realize that their private and personal data are being collected as they browse the website.<sup>11</sup>

110. Tracking Pixels may collect various types of information, including sensitive information and less sensitive information.

---

<sup>9</sup> *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FTC (Mar. 16, 2023), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking> [<https://perma.cc/Y8TJ-53FD>].

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*

111. Some Tracking Pixels harvest data regarding website users' entertainment or shopping habits and preferences.

112. In this case, the Tracking Pixels embedded in Defendants' Website do not merely collect shopping trends or similar commercial data; instead, Defendants' Tracking Pixels collect highly sensitive, personal health-related information.

113. Traditional methods of preventing web-browsing data from being collected, such as blocking third-party cookies, may not prevent Tracking Pixels from collecting user data. As a result, users may have no effective way to block the collection of their private information by Tracking Pixels.<sup>12</sup>

114. While some Tracking Pixel providers claim that they attempt to remove personal information from the data they collect, these efforts are not always successful.

115. For example, the Federal Trade Commission ("FTC") has said that methods such as "hashing" personal information to scramble it may be inadequate.<sup>13</sup>

116. Session Replay Code operates similarly to Tracking Pixels, often relying on network traffic requests to transmit recorded interaction data.

117. However, Session Reply Code extracts even more intrusive details about users' browsing behavior.

---

<sup>12</sup> *Id.*

<sup>13</sup> *Id.*; Ed Felten, *Does Hashing Make Data "Anonymous"?*, FTC (Apr. 22, 2012), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2012/04/does-hashing-make-data-anonymous> [<https://perma.cc/5UMN-UZR4>].

118. Specifically, Session Replay Code logs and tracks *everything* a user does on a webpage, including mouse movements, clicks, scrolls, and taps, and can actually track every single key stroke, creating a *complete* reproduction of the user's visit to the website.<sup>14</sup>

119. Network traffic requests are also often used by tracking pixels and session replay tools to send user data back to third-party servers.

### **III. Confidential Personal Health Data Covertly Obtained from Websites Presents Serious Privacy Risks**

120. Data pertaining to individuals are so valuable they have been compared to the “new oil.”<sup>15</sup>

121. However, the market for such data, and in particular personal health-related data, presents serious privacy risks.

122. For this reason, Time Magazine has pointed out that the health data market, while highly lucrative, poses a significant risk to individuals' privacy.<sup>16</sup>

123. Nevertheless, the enormous value of personal health data incentivizes businesses to use invasive tracking technologies on their websites to collect these data from website users.

---

<sup>14</sup> *The Definitive Guide to Session Replay*, FULLSTORY (Oct. 8, 2024), <https://www.fullstory.com/blog/session-replay/> [<https://perma.cc/56WH-8GQ5>].

<sup>15</sup> *The World's Most Valuable Resource Is No Longer Oil, but Data*, THE ECONOMIST (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> [<https://perma.cc/US3V-CPCU>].

<sup>16</sup> Adam Tanner, *How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry*, TIME (Jan. 9, 2017, 9:00 AM), <https://time.com/4588104/medical-data-industry/> [<https://perma.cc/F3WR-HHVL>].

124. For example, the data collected by Tracking Pixels are valuable to businesses because they can use them to track Internet users and target ads based on prior browsing behavior.<sup>17</sup> This practice can be highly lucrative.

125. As one report explained, “There’s a whole market of brokers who compile the [personal health] data from providers and other health-care organizations and sell it to buyers.”<sup>18</sup>

126. According to a report from cybersecurity company Feroot Security, “medical-related websites continue to be mined for data including personal medical information[.]”<sup>19</sup>

127. As early as 2015, experts were researching how confidential health information is shared with third parties without users’ knowledge.<sup>20</sup>

128. In June 2022, an investigation by The Markup<sup>21</sup> revealed that one Tracking Pixel, the Meta Pixel, collected and sent a “data packet” to Facebook whenever a user engaged with some hospital websites, such as clicking to schedule a doctor’s appointment.

---

<sup>17</sup> *Id.*

<sup>18</sup> Christina Farr, *Hospital Execs Say They Are Getting Flooded with Requests for Your Health Data*, CNBC (Dec. 18, 2019, 8:27 AM), <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html> [<https://perma.cc/D7CL-N3HX>].

<sup>19</sup> *Private Health Data Still Being Exposed to Big Tech, Report Says*, INSURANCE JOURNAL (Oct. 17, 2023), <https://www.insurancejournal.com/news/national/2023/10/17/744625.htm> [<https://perma.cc/M8YP-WDKU>].

<sup>20</sup> Timothy Libert, *Privacy Implications of Health Information Seeking on the Web*, COMMUNICATIONS OF THE ACM (March, 2015), [https://timlibert.me/pdf/Libert-2015-Health\\_Privacy\\_on\\_Web.pdf](https://timlibert.me/pdf/Libert-2015-Health_Privacy_on_Web.pdf) [<https://perma.cc/NC4F-5GRZ>].

<sup>21</sup> *Facebook is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP, <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites> [<https://perma.cc/3X7W-MMJB>].

129. Further research by The Markup revealed that the personal health data transmitted to Facebook by the Meta Pixel from hospital websites included not only sensitive health information, such as details about medications, allergies, and upcoming doctor visits, but also personally identifiable information, including patients' names, addresses, email addresses, and phone numbers.

130. Additionally, The Markup's investigation found that the Meta Pixel was embedded in public-facing hospital websites and within password-protected patient portals at seven health systems, including FastMed and Novant Health.<sup>22</sup>

131. The FTC has taken enforcement action against Internet providers who track sensitive health data.

132. For example, in June 2022, the FTC finalized a settlement with Facebook regarding its covert collection of sensitive medical data when Flo, an ovulation tracking app, shared users' private health information with Facebook<sup>23</sup> and other advertisers.<sup>24</sup>

---

<sup>22</sup> *Id.*

<sup>23</sup> *FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others*, FTC (Jun 22, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google> [<https://perma.cc/V33W-LEEE>].

<sup>24</sup> Justin Sherman, *Your Health Data Might Be for Sale*, SLATE (Jun 22, 2022, 5:50 AM), <https://slate.com/technology/2022/06/health-data-brokers-privacy.html> [<https://perma.cc/L7U4-4VMW>].

#### **IV. The Unauthorized Collection of Personal Health Data Contravenes Legal, Ethical, and Social Norms**

##### **A. Website Users Reasonably Expect Personal Health Information to Be Confidential**

133. Personal health data collected by Tracking Pixels, Session Replay Code, and other tracking technologies may be “highly personal information that people choose not to disclose even to family, friends, or colleagues,” which nevertheless “is actually shared with complete strangers.”<sup>25</sup>

134. According to the FTC, personal health information is “[a]mong the most sensitive categories of data collected by connected devices[.]”<sup>26</sup>

135. Personal health information collected by websites “may pose an incalculable risk to personal privacy.”<sup>27</sup> The practice of allowing Third-Party Vendors to “collect that data, combine it, and sell or monetize it” would be an “unprecedented intrusion.”<sup>28</sup> That is exactly what Defendants have done, and are doing.

136. Consumers’ confidence that their personal and private health data will be kept secure is a major public health issue.

137. A 2015 review found that “the social stigma associated with some health conditions is among the top reasons consumers delay or avoid getting help

---

<sup>24</sup> Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data*, FTC (July 11, 2022) <https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal> [<https://perma.cc/67CF-PZ3Y>].

<sup>26</sup> *Id.*

<sup>27</sup> *Id.*

<sup>28</sup> *Id.*

for mental health problems.”<sup>29</sup>

138. The fear of “disclosure and confidentiality concerns” was a prominent cause of this stigma.<sup>30</sup>

139. Once a person’s private and sensitive health information is available, it exposes that individual to significant harm.

140. Personal health data are used by criminals and other malevolent actors to facilitate phishing scams, commit identity theft, and inflict physical or emotional injury.<sup>31</sup>

141. Information about private health and medical matters, especially data related to sexual activity or reproductive health, “may subject people to discrimination, stigma, mental anguish, or other serious harms.”<sup>32</sup>

**B. Personal Health Information Can Be Harvested for Commercial Gain**

142. Companies that collect personal information “have a profit motive to share data at an unprecedented scale and granularity.”<sup>33</sup>

143. Once an individual’s personal and private health data are collected, they “often have no idea who has it or what’s being done with it.”

---

<sup>29</sup> *Report: Companies Continue to Share Health Data Despite New Privacy Laws*, CONSUMER REPORTS (Jan. 16, 2024), <https://advocacy.consumerreports.org/wp-content/uploads/2024/01/Companies-Continue-to-Share-Health-Data-1-16-2024-Consumer-Reports.pdf> [<https://perma.cc/7WFB-BBTW>].

<sup>30</sup> *Id.*

<sup>31</sup> Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data*, FTC (July 11, 2022) <https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal> [<https://perma.cc/67CF-PZ3Y>].

<sup>32</sup> *Id.*

<sup>33</sup> *Id.*

144. The data “enters a vast and intricate sales floor frequented by numerous buyers, sellers, and sharers.”<sup>34</sup>

145. In a 2014 study, the FTC reported that data brokers use data collected from consumers to create profiles that may contain sensitive inferences, such as categorizing someone as an “expectant parent.”<sup>35</sup>

146. Once these invasive and sensitive profiles have been created, the brokers use them to track visitors across the Internet with “personalized” ads.<sup>36</sup>

147. The categories that consumers are placed into can be incredibly private or invasive, such as “working-class mom,” “frequent alcohol drinker,” “financially challenged,” or “depression sufferer.”<sup>37</sup>

148. In the same 2014 study, one data broker, Acxiom, bragged to shareholders that it had 3,000 points of data for nearly every consumer in the United States.<sup>38</sup>

---

<sup>34</sup> *Id.*

<sup>35</sup> *Id.*; *Data Brokers: A Call For Transparency and Accountability: A Report of the Federal Trade Commission*, FTC (May 2014), <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf> [<https://perma.cc/M6QR-5LXA>].

<sup>36</sup> *Id.*

<sup>37</sup> *Online Advertising & Tracking*, EPIC, <https://epic.org/issues/consumer-privacy/online-advertising-and-tracking/> [<https://perma.cc/GX3W-67XS>].

<sup>38</sup> *Data Brokers: A Call For Transparency and Accountability: A Report of the Federal Trade Commission*, FTC (May 2014), <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf> [<https://perma.cc/M6QR-5LXA>]; Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data*, FTC (July 11, 2022) <https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal> [<https://perma.cc/67CF-PZ3Y>].

149. Data aggregators and brokers gather this collected personal data and “sell access to it (or analyses derived from it) to marketers, researchers, and even government agencies.”<sup>39</sup>

150. The scale of the personal and private data flowing from users to brokers is staggering.

151. The sheer number of ads shown to Internet users is overwhelming, with Americans exposed to an estimated 5,000 ads daily.<sup>40</sup>

152. According to the FTC, “some popular ad exchanges can handle tens of billions of auctions per day. Each auction involves a broadcast of consumer data being sent to potentially dozens of bidders simultaneously, despite only one of those parties – the winning bidder – actually using these data to serve a targeted ad.”<sup>41</sup>

153. Once private and personal data are in the hands of data brokers, “there are few (if any) technical controls ensuring that [they] do not retain that data for use in unintended ways.”<sup>42</sup>

**C. Regulatory Authorities Prohibit the Unauthorized Collection and Tracking of Private Health Information**

154. Elevance and Anthem, as health insurance issuers and providers of health plans (including employer-sponsored group health plans), are both considered to be “covered entit[ies]” under HIPAA.

---

<sup>39</sup> *Id.*

<sup>40</sup> *Online Advertising & Tracking*, EPIC, <https://epic.org/issues/consumer-privacy/online-advertising-and-tracking/> [<https://perma.cc/GX3W-67XS>].

<sup>41</sup> *Unpacking Real Time Bidding through FTC’s case on Mobilewalla*, FTC (Dec. 3, 2024), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/12/unpacking-real-time-bidding-through-ftcs-case-mobilewalla> [<https://perma.cc/8WYU-UPGW>].

<sup>42</sup> *Id.*

155. The U.S. Department of Health and Human Services (“HHS”) has issued a bulletin covering the use of online tracking technologies, such as Tracking Pixels and Session Replay Code, by these HIPAA-covered entities. The bulletin clarifies the privacy and security rules promulgated under HIPAA, 42 U.S.C. §§ 1320d–1320d-9.

156. The HHS bulletin states that “[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of [PHI] to tracking technology vendors or any other violations of the HIPAA rules.”<sup>43</sup>

157. The bulletin continues, “[f]or example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals’ HIPAA-compliant authorizations, would constitute impermissible disclosures.”<sup>44</sup>

158. The bulletin further explains that the PHI collected by tracking technologies placed on websites, such as Tracking Pixels and Session Replay Code, can include “an individual’s medical record number, home or email address, or dates of appointments, as well as an individual’s IP address or geographic location, device IDs, or any unique identifying code.”<sup>45</sup>

159. Defendants’ use of tracking technologies on the Website, such as Tracking Pixels, violates HHS’s bulletin, which explicitly states that regulated

---

<sup>43</sup> *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, HHS, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (last updated June 26, 2024) [<https://perma.cc/8CCZ-49SW>].

<sup>44</sup> *Id.*

<sup>45</sup> *Id.*

entities like Defendants are not permitted to use tracking technologies in ways that lead to impermissible disclosures of PHI to third parties without obtaining HIPAA-compliant authorizations.

160. The HHS bulletin further clarifies that disclosure of PHI to vendors for marketing purposes (including targeted advertising or analytics used to improve advertising performance) violates HIPAA without HIPAA-compliant authorization from the individual.

161. Defendants' conduct, including enabling Third-Party Vendors to track insureds on Defendants' Website for advertising purposes, is exactly the type of unauthorized data sharing of sensitive medical information that the HHS bulletin states is prohibited.

162. On user-authenticated websites, which require a user to log in before gaining access to the site, tracking technologies may "have access to an individual's diagnosis and treatment information, prescription information, billing information, or other information within the portal."<sup>46</sup>

163. Even on unauthenticated websites, which do not require users to log in before gaining access to the website, tracking technologies may obtain access to an individual's PHI.

164. The HHS bulletin gives the following example: "[I]f an individual were looking at a hospital's webpage listing its oncology services to seek a second opinion on treatment options for their brain tumor, the collection and transmission of the

---

<sup>46</sup> *Id.*

individual's IP address, geographic location, or other identifying information showing their visit to that webpage is a disclosure of PHI to the extent that the information is both identifiable and related to the individual's health or future health care.”<sup>47</sup>

165. The HHS bulletin outlines the harms that disclosure of PHI may cause, including “identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI.”<sup>48</sup>

166. The disclosure of an individual's PHI “can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.”<sup>49</sup>

167. In a joint letter sent on July 23, 2023, to hospital systems and telehealth providers, the FTC and the HHS Office for Civil Rights also reiterated the risks posed by the disclosure of an individual's personal health information to third parties.

168. The joint letter noted that such disclosures could reveal “sensitive information including health conditions, diagnoses, medications, medical

---

<sup>47</sup> *Id.*

<sup>48</sup> *Id.*

<sup>49</sup> *Id.*

treatments, frequency of visits to health care professionals, and where an individual seeks medical treatment.”<sup>50</sup>

169. At the state level, Indiana grants protections for medical records, including Indiana Code § 16-39-5-3(f)–(h) (patient identity is confidential, even when used for research purposes), 410 IAC 1-2.5-78 (criminal penalties for intentional disclosure of medical information), and Indiana Code § 16-39-2-6 (confidentiality of mental health records).

170. The American Medical Association’s (“AMA”) *Code of Medical Ethics* also promulgates rules that protect the privacy of patient data and communications.

171. These AMA rules include, but are not limited to, *AMA Code of Medical Ethics* Opinion 3.1.1 (“[p]atient privacy encompasses a number of aspects, including . . . personal data”), Opinion 3.2.4 (“Information gathered and recorded in association with the care of the patient is confidential.”), and Opinion 3.3.2 (“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.”).

## **V. Confidentiality Expectations in Member Portals**

172. Password-protected portals are subpages of a health insurer’s website to which users gain access only after registering, verifying identity, and logging in with credentials.

---

<sup>50</sup> *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, FTC (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> [<https://perma.cc/EB3S-UF3V>].

173. These portals typically provide individualized services to users, including the ability to research medical and health issues, view insurance claims, obtain explanations of benefits, track insurance deductibles, review prescriptions, and update member profile information.<sup>51</sup>

174. Portals function as live dashboards, providing, among other things, updates on claims, prescriptions, lab results, and secure messaging. Because these updates are continuous, portal activity creates a detailed summary of an individual's health. Studies show that increased portal use is associated with better health outcomes.<sup>52</sup>

175. Portal content is nonpublic and tailored to each insured; it is not accessible to anonymous website visitors.

176. Because portal interactions are tied to a specific user's identity, the data displayed or transmitted often constitutes individually identifiable health information ("IIHI"), a category of PHI under HIPAA. 45 C.F.R. § 160.103.

177. From a user's perspective, logging into a portal signals entry into a private communication channel with the insurer in which there is an expectation that health information shared in the portal will be kept confidential.<sup>53</sup>

---

<sup>51</sup> Courtney R. Lyles, Janey Hamblin, Victor Y.X. Lin, Dean Schillinger, *Legal, Practical, and Ethical Considerations for Making Online Patient Portals Accessible for All*, 107 Am. J. Pub. Health 1608 (2017), available at <https://pmc.ncbi.nlm.nih.gov/articles/PMC5607665/pdf/AJPH.2017.303933.pdf> [<https://perma.cc/U52A-RE2Q>].

<sup>52</sup> *Id.*

<sup>53</sup> *K.L. v. Legacy Health*, No. 23-1886, 2024 U.S. Dist. LEXIS 206864, at \*9 (D. Or. Nov. 14, 2024).

**VI. Defendants Covertly Intercepted Plaintiffs' Sensitive Health Information for Commercial Profit**

**A. Defendants Covertly Wiretapped Website Communications**

178. Despite deep public concerns about Internet privacy and the sensitivity of personal health-related data, Defendants unlawfully embedded code in the Website that allows Third-Party Vendors to harvest, for financial benefit, the sensitive private health information of Defendants' insureds.

179. Defendants also benefit from the Tracking Technologies on the Website, because the data generated by these Tracking Technologies allow Defendants to identify groups or segments among their insureds, and refine marketing to increase enrollment and revenue.

**B. Defendants' Enabling of Quantum Metric's Tracking Technology on Defendants' Purportedly "Secure" Patient Portals**

**1. Quantum Metric's Role and Capabilities**

180. Defendants have embedded the Tracking Technologies of Third-Party Vendor Quantum Metric within their purportedly secure patient portals in order to enable the interception and collection of users' private data and communications, including health-related queries, without user consent. The code begins tracking immediately after users enter their usernames and passwords and log in to the portals.

181. Quantum Metric is a digital analytics (i.e., marketing) service that captures user interaction data.<sup>54</sup> It provides a Digital Experience Analytics (“DXA”) platform, marketed as “[capturing] insight from 40% of the world’s internet users.”<sup>55</sup>

182. DXA captures performance metrics like click-through rates with session replay and heatmaps; as Quantum Metric explains, “[f]eatures like detailed session replays (showing exact user actions), heatmaps (visualizing popular areas on a page), and automatic ‘friction detection’ (spotting where users struggle) are becoming standard to truly understand how customers *feel* when using your digital services.”<sup>56</sup>

183. Of note, Quantum Metric’s tools are specifically advertised as allowing for tracking in real time, with the company stating that “real-time insights are crucial” and “this means looking at every single user interaction as it happens, not days later.”<sup>57</sup>

184. Quantum Metric’s Tracking Technologies are embedded throughout Defendants’ Website, including in purportedly secure portals, and track users in real time. The figure below and the other figures in this Complaint that contain code were captured using the Chrome browser’s developer tools, which allow real-

---

<sup>54</sup> *Quantum Metric Recognized as Top Digital Experience Analytics Platform*, QUANTUM METRIC, <https://www.quantummetric.com/resources/digital-experience-analytics-platforms-matrix> [<https://perma.cc/KUW7-BW8T>].

<sup>55</sup> *Key DXA Trends Shaping the Market*, QUANTUM METRIC, <https://www.quantummetric.com/events/key-dxa-trends-shaping-the-market> [<https://perma.cc/N6YH-JVTB>].

<sup>56</sup> Quantum Metric, *What is Digital Experience Analytics? Your 2025 Guide* (Jul. 10, 2025), <https://www.quantummetric.com/blog/digital-experience-analytics-2025-guide> [<https://perma.cc/QHZ2-7EPS>].

<sup>57</sup> *Id.*

time observation of the data a website sends and receives when visited. These figures show what data a user's browser is sending and receiving in real time.

|                                  |                                                                                                                                                            |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ▼ General                        |                                                                                                                                                            |
| Request URL                      | https://ingest.quantummetric.com/horizon/anthem?T=B&u=http:ber%2Fdashboard&t=1759435318495&v=1759435403249&H=3:77bea30f543d17ee&p=8&N=8&S=9198367&b=20&z=1 |
| Request Method                   | POST                                                                                                                                                       |
| Status Code                      | 200 OK                                                                                                                                                     |
| Remote Address                   | 34.8.9.231:443                                                                                                                                             |
| Referrer Policy                  | no-referrer-when-downgrade                                                                                                                                 |
| ▼ Response Headers               |                                                                                                                                                            |
| Access-Control-Allow-Credentials | true                                                                                                                                                       |
| Access-Control-Allow-Origin      | https://membersecure.anthem.com                                                                                                                            |
| Alt-Svc                          | h3=":443"; ma=2592000,h3-29=":443"; ma=2592000                                                                                                             |
| Content-Length                   | 0                                                                                                                                                          |
| Content-Type                     | application/json                                                                                                                                           |
| Date                             | Thu, 02 Oct 2025 20:03:23 GMT                                                                                                                              |
| Strict-Transport-Security        | max-age=31536000; includeSubDomains                                                                                                                        |
| Via                              | 1.1 google                                                                                                                                                 |
| ▼ Request Headers                |                                                                                                                                                            |
| :authority                       | ingest.quantummetric.com                                                                                                                                   |
| :method                          | POST                                                                                                                                                       |
| :path                            | /horizon/anthem?                                                                                                                                           |

*Figure 1*

## 2. Quantum Metric's Session Replay Code Inside Portal

185. As the patient portal landing page loads, Quantum Metric's tracking script loads simultaneously. As shown in Figure 1, the browser issues a network traffic request (a message sent by the browser to ask for data) to https://ingest.quantummetric.com, a custom domain designed to import data to Quantum Metric servers for analytics processing. This script loads even before the user takes any action in the portal.

186. Once loaded, the Quantum Metric script executes in the user's browser, enabling real-time monitoring of all user interactions. This includes tracking typed entries, mouse movements, clicks, scrolling behavior, page

navigation, and the content of Website Communications, such as search queries.

The script transmits this information directly to Quantum Metric’s servers.

187. For instance, Quantum Metric’s tracking technologies intercept user data when a user performs a “benefits search” within the patient portal and selects the filter “mental health,” which returns a variety of hyperlinked facilities within Defendants’ provider network for users to explore. As shown in Figure 2 below, Quantum Metric’s Tracking Technologies continue to intercept user interactions as the user navigates through specific provider subpages:

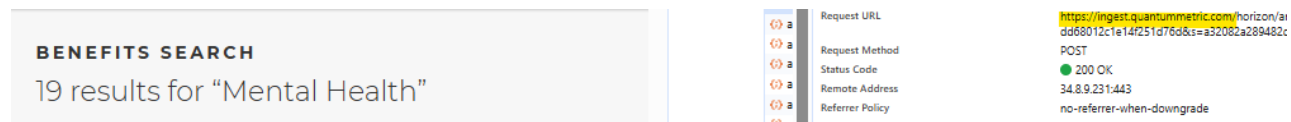
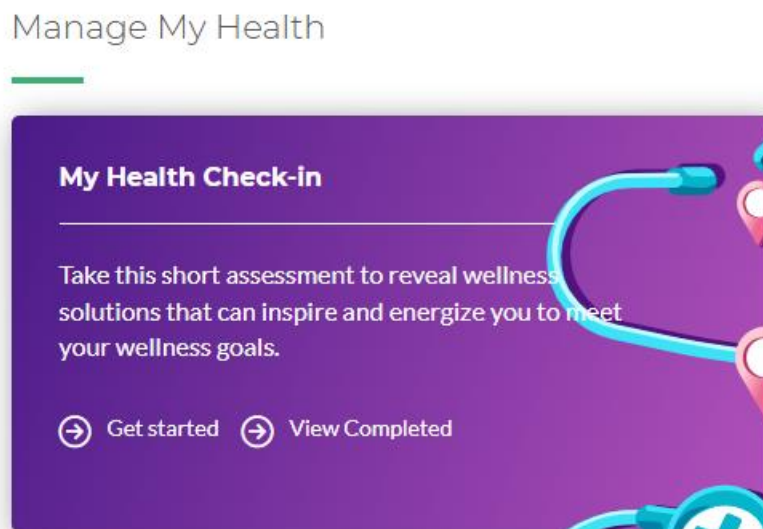


Figure 2

188. As shown in Figure 3 below, the “Manage My Health” tool within the patient portal prompts users to complete a short assessment (“My Health Check-in”) composed of highly sensitive questions pertaining to users’ medical, financial,



and emotional needs in order to “reveal wellness solutions that can inspire and energize you to meet your wellness goals:”

*Figure 3*

189. As shown in Figure 4 below that shows what the Website user sees as they browse (and the associated input of personal content like “I’m worried about having enough money”), and Figure 5 that shows what data are simultaneously being transmitted, these interactions are intercepted by the Quantum Metric analytics domain, which assigns each user session an embedded hashed identifier (e.g., “&s=” and following string). The resulting network traffic request transmits information about the user’s session – including sensitive personal statements such as “I’m worried about having enough money” – to ingest.quantummetric.com:

15%

Last Saved at 1:59 PM October 01, 2025

☐ I'm concerned about medical treatment, my condition, or my symptoms

☐ I want to be healthier and prevent sickness

☒ I'm worried about having enough money

☐ I want to get the most out of my health insurance

What concerns you most? (Check all that apply)

☒ Can't afford rent or house payment

☐ A place to live

☐ Unemployment or looking for a job

☐ Can't pay for groceries, gas, basics

☐ Paying doctor bills

☐ Paying for my prescriptions

☐ Other, please specify

☐ Decline to answer

Are you worried about losing your housing?

☒ Yes

☐ No

☐ Decline to answer

Do you have any of these conditions? (Check all that apply)

☐ No conditions, feeling fine

☐ Asthma, bronchitis

☐ Arthritis, joint disorders

☒ Bipolar disorders

Feedback

Chat With Us

*Figure 4*

|                                  |                                                                                                                                                                                                                                                                                 |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ▼ General                        |                                                                                                                                                                                                                                                                                 |
| Request URL                      | https://ingest.quantummetric.com/horizon/anthem?T=B&u=https%3A%2F%2Fmembersecure.anthem.com%2Fmember%2Fmy-health-dashboard%2Fmanage-my-health%2Fwelcome%3D*****%2&v=1759517591053&s=bd54bd109afd1e6febef2725a67e3b5Q=1&Y=1&X=b6df4a6fc1b84d5b24e36484448c8157&S=0&b=884706&cz=1 |
| Request Method                   | POST                                                                                                                                                                                                                                                                            |
| Status Code                      | 200 OK                                                                                                                                                                                                                                                                          |
| Remote Address                   | 34.8.9.231:443                                                                                                                                                                                                                                                                  |
| Referrer Policy                  | no-referrer-when-downgrade                                                                                                                                                                                                                                                      |
| ▼ Response Headers               |                                                                                                                                                                                                                                                                                 |
| Access-Control-Allow-Credentials | true                                                                                                                                                                                                                                                                            |
| Access-Control-Allow-Origin      | https://membersecure.anthem.com                                                                                                                                                                                                                                                 |
| Alt-Svc                          | h3=":443"; ma=2592000,h3-29=":443"; ma=2592000                                                                                                                                                                                                                                  |
| Content-Length                   | 0                                                                                                                                                                                                                                                                               |
| Content-Type                     | application/json                                                                                                                                                                                                                                                                |
| Date                             | Fri, 03 Oct 2025 18:53:11 GMT                                                                                                                                                                                                                                                   |
| Strict-Transport-Security        | max-age=31536000; includeSubDomains                                                                                                                                                                                                                                             |
| Via                              | 1.1 google                                                                                                                                                                                                                                                                      |
| ▼ Request Headers                |                                                                                                                                                                                                                                                                                 |
| :authority                       | ingest.quantummetric.com                                                                                                                                                                                                                                                        |

Figure 5

190. Quantum Metric intercepts this information despite Defendants’ representations, set forth in Figure 6 below, that user answers are “never shared with third parties:”

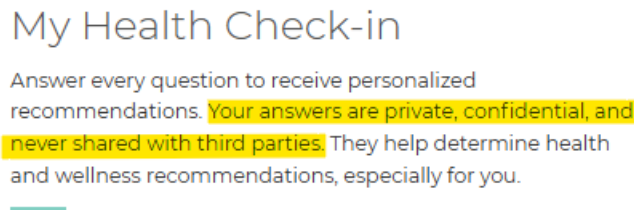


Figure 6<sup>58</sup>

191. By recording and reproducing the entirety of users’ interactions (including searches, form entries, and navigation), Quantum Metric captures PHI along with other sensitive health-related data and information.

<sup>58</sup> Because this page resides in Defendants’ secure online portal, there is no hyperlink for citation or review in this pleading.

**C. Defendants’ Enabling of Medallia’s Tracking Technology on Defendants’ Website, Including in Purportedly “Secure” Patient Portals**

1. Medallia’s Role and Capabilities

192. Defendants have embedded the Tracking Technologies of Third-Party Vendor Medallia within their purportedly secure patient portals in order to enable the interception and collection of users’ private data and communications, including health-related queries, without user consent.

193. The code begins tracking immediately after users enter their usernames and passwords and log in to the portal.

194. Medallia is a private software company that provides tracking and analytical tools that record how users interact with websites in real time.

195. Medallia creates session replays, allowing its clients to watch recordings of users’ visits, and it also generates “heatmaps” to show where users clicked or hesitated.<sup>59</sup>

196. Medallia explicitly markets its tool as a way to “visualize every visitor’s digital experience . . . from what they did (e.g., clicks) to what they saw (e.g., pop-ups).”<sup>60</sup>

197. Medallia is one of the most active third-party data recipients on Anthem’s website, and its analytics request usually executes via the domain of analytics-fe.digital-cloud-west.medallia.com.

---

<sup>59</sup> *Heatmaps*, MEDALLIA, <https://www.medallia.com/products/digital-experience-analytics/heatmaps/n> [https://perma.cc/MC8P-AHZ8].

<sup>60</sup> *Session Replay*, MEDALLIA, <https://www.medallia.com/products/digital-experience-analytics/session-replay/> [https://perma.cc/SQ9C-9TWF].

198. Medallia's embedded code in Defendants' Website harvests detailed personal and private information of users of Defendants' Website, including the exact keywords searched and other user interactions with the Website.

199. Medallia obtained the highly sensitive health-related information of users of Defendants' Website with the intent of using the information it obtained for commercial gain through targeted advertising.

## 2. Medallia's Code Operates Inside Patient Portals

200. Medallia's Tracking Technologies are embedded throughout Defendants' Website, including in purportedly secure portals, and track users in real time. The following figure illustrates how Medallia's embedded code operates:

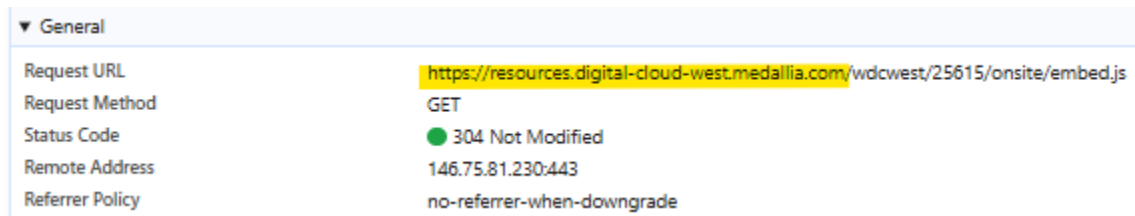


*Figure 7*

201. The above screenshot shows how, as the patient portal landing page loads, Medallia's tracking script loads simultaneously. The browser issues a network traffic request to <https://resources.digital-cloudwest.medallia.com/wdcwest/25615/onsite/embed.js>, a custom JavaScript file hosted and controlled by Medallia.

202. Once loaded, the Medallia script executes in the user's browser, enabling real-time monitoring of all user interactions. This includes tracking typed entries, mouse movements, clicks, scrolling behavior, page navigation, and the

content of Website Communications, such as search queries. The script transmits this information directly to Medallia’s servers.

203. This demonstrates that Medallia’s script loads alongside core portal functions, capturing patient interactions at the moment they occur.

204. When a user visits the “Prescription” tab of the patient portal, which allows users to view and manage prescriptions, the browser executes a network traffic request to the Medallia domain displayed in Figure 8 with a series of embedded cookies:

Request Cookies ☒ show filtered out request c...

| Name             | Value            | Domain        |
|------------------|------------------|---------------|
| __q_state_1aA... | eyJ1dWlkjoiM...  | .medallia.com |
| _biz_flagsA      | %7B%22Versi...   | .medallia.com |
| _biz_nA          | 4                | .medallia.com |
| _biz_pendingA    | %5B%5D           | .medallia.com |
| _biz_uid         | 122a699b36dc...  | .medallia.com |
| _fbp             | fb.1.17537184... | .medallia.com |
| _ga              | GA1.1.109129...  | .medallia.com |
| _ga_QPF6JLZL2T   | GS2.1.s175373... | .medallia.com |
| _gcl_au          | 1.1.500021845... | .medallia.com |
| _mkto_trk        | id:141-HJW-8...  | .medallia.com |
| _one_Mzc3MD...   | 82b8d3f5-baa...  | .medallia.com |
| _zitok           | 75f5e5227bc6...  | www.meda...   |
| AMCV_28F958...   | MCMID 01499...   | .medallia.com |
| da_lid           | EDE9107F9A6...   | .medallia.com |
| kndctr_28F958... | CiYwMTQ5OT...    | .medallia.com |

Figure 8<sup>61</sup>

205. As shown in the above screenshot, several tracking cookies operated by Google Ads (\_gcl\_au), Adobe Experience Cloud (AMCV\_28F958..) and Facebook/Meta Pixel (\_fbp) remain during the user’s session and store unique user identifiers, seen in the “Value” column, before users’ session information is sent to a

<sup>61</sup> Figure 8 was captured from a live browser session and it displays the active third-party tracking cookies (small tracking files that allow third parties to follow what a user does on the site and connect that activity to a unique ID) that load when a user logs in.

.medallia.com domain, thereby enabling third parties like Medallia to reasonably associate a user ID with a specific prescription interaction.

206. This shows how Medallia correlates patient portal activity, such as prescription management, with unique user identifiers.

207. The following code from Defendants' Website shows how highly sensitive, private, personal data – in this case migraines, indicating the user is likely suffering from the condition – are intercepted by Medallia on the Website's main search bar:

| ▼ General                   |                                                                                                                  |
|-----------------------------|------------------------------------------------------------------------------------------------------------------|
| Request URL                 | https://resources.digital-cloud-west.medallia.com/wdcwest/28145/onsite/generic1753631507399.js                   |
| Request Method              | GET                                                                                                              |
| Status Code                 | 200 OK                                                                                                           |
| Remote Address              | 146.75.81.230:443                                                                                                |
| Referrer Policy             | strict-origin-when-cross-origin                                                                                  |
| ▼ Response Headers          |                                                                                                                  |
| Accept-Ranges               | bytes                                                                                                            |
| Access-Control-Allow-Origin | *                                                                                                                |
| Age                         | 786541                                                                                                           |
| Cache-Control               | max-age=2592000                                                                                                  |
| Content-Encoding            | gzip                                                                                                             |
| Content-Length              | 85220                                                                                                            |
| Content-Type                | application/javascript                                                                                           |
| Date                        | Tue, 05 Aug 2025 18:20:49 GMT                                                                                    |
| Etag                        | "cf9f3f3c2674e1525d13f7a83e23504c"                                                                               |
| Last-Modified               | Sun, 27 Jul 2025 15:51:48 GMT                                                                                    |
| Server                      | AmazonS3                                                                                                         |
| Strict-Transport-Security   | max-age=31557600                                                                                                 |
| Vary                        | Accept-Encoding                                                                                                  |
| Via                         | 1.1 varnish                                                                                                      |
| X-Amz-Id-2                  | 9FQA86hoQB8no8PnhQJurf4r2IUJVG9oXTKVtFvsx/05WOrmLBdBZFtgLjMebDB7/lxk+tDrGp6ecgq9hVSUrKT<br>r+1ic7CA9whm/fLDdSA8= |

*Figure 9*

208. The above screenshot shows how, after the user searches for “migraines,” Defendants’ Website loads third-party tracking code from Medallia by issuing a network traffic request to a Medallia-controlled domain, <https://resources.digital-cloud-west.medallia.com>. This request retrieves and executes a JavaScript file, as shown by the “Content-Type” referring to JavaScript.

209. This confirms that Medallia’s code executes directly in response to a patient’s health-related query.

```

-      }
50      KAMPYLE_DATA.setMemoryData('isSyncedIdentifierData', false);
-      KAMPYLE_DATA.setData('kampyleUserSession', KAMPYLE_UTILS.get(
-      KAMPYLE_DATA.setData('kampyleSessionPageCounter', 0);
-      addToSessionCount();
-      KAMPYLE_DATA.deleteData('kampyleUserPercentile');
-      KAMPYLE_DATA.deleteData('kampyleInvitePresented');
-      KAMPYLE_DATA.deleteData(KAMPYLE_CONSTANT.SESSION_DATA_FIELDS.
-      if (!checkProvision(KAMPYLE_CONSTANT.PROVISIONS.DISABLE_USER_
-      KAMPYLE_TARGETING.setUserPercentile();
-      }
51      if (window.MDIGITAL.ANALYTICS && KAMPYLE_FUNC.checkProvision(
-      MDIGITAL.ANALYTICS.triggerDigitalAnalyticsEvent('neb_sess
-      additionalData: sessionData
-      });
-      }
-    }

```

*Figure 10*

210. As shown in the above screenshot, the JavaScript file retrieved from Medallia enables session replay functionality, with instructions to transmit user data. The script sets a unique session identifier (kampyleUserSession) and tracks user engagement by counting page views (kampyleSessionPageCounter).

211. The code in Figure 10 further includes commands to trigger digital analytics events, such as the command MDIGITAL.ANALYTICS.trigger

DigitalAnalyticsEvents, which transmits these data in real time to third parties like Medallia.

212. In this way, Medallia’s session replay functionality extends beyond metadata to capture the content of users’ interactions inside the portal. It includes the actual content of any searches, like for “Migraines,” as shown in Figure 11.

|                 |                                                                                                                                                                                                                                                        |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| :authority      | resources.digital-cloud-west.medallia.com                                                                                                                                                                                                              |
| :method         | GET                                                                                                                                                                                                                                                    |
| :path           | /wdcwest/28145/onsite/generic1753631507399.js                                                                                                                                                                                                          |
| :scheme         | https                                                                                                                                                                                                                                                  |
| Accept          | */*                                                                                                                                                                                                                                                    |
| Accept-Encoding | gzip, deflate, br, zstd                                                                                                                                                                                                                                |
| Accept-Language | en-US,en;q=0.9                                                                                                                                                                                                                                         |
| Cache-Control   | no-cache                                                                                                                                                                                                                                               |
| Cookie          | AMCV_28F958C45FF3799D0A495C47%40AdobeOrg=MC<br>MID 1611122973817773106405465433054875428;<br>kndctr_28F958C45FF3799D0A495C47_AdobeOrg_identity<br>=CiYxNjExMTlyOTczODE3NzczMTA2NDA1NDY1NDMzMz<br>A1NDg3NTQyOFIQJHSxdr%2DMhgBKgNPUjIwAfAB79i%<br>5FrYcz |
| Pragma          | no-cache                                                                                                                                                                                                                                               |

*Figure 11*

213. The above screenshot additionally shows that Defendants place a tracking cookie on Website users’ browsers that sends their personal, highly sensitive private data to Medallia.

214. The cookie (as shown in Figure 11) also assigns a unique identifier to that user’s device, allowing Defendants and the Third-Party Vendors to identify and monitor users across sessions and webpages, and to build a behavioral profile.

215. Thus, Medallia’s tracking is not limited to a single visit but enables ongoing surveillance tied to the same individual.

216. In addition to the network traffic request outlined above that retrieves and runs Medallia’s scripts, Medallia initiates network traffic requests that transmit the content of users’ health queries directly to Medallia, as shown in Figure 12:

| ▼ General       |                                                                     |
|-----------------|---------------------------------------------------------------------|
| Request URL     | https://analytics-fe.digital-cloud-west.medallia.com/api/web/events |
| Request Method  | POST                                                                |
| Status Code     | ● 200 OK                                                            |
| Remote Address  | 147.75.243.60:443                                                   |
| Referrer Policy | strict-origin-when-cross-origin                                     |

*Figure 12*

217. This network traffic request explicitly refers to the *full and exact* search query made by a user on Defendants’ Website, with data transmitted to Medallia indicating that the user’s search concerned migraines, as the search URL was “https://www.anthem.com/search/?q=migraines,” as shown in Figure 13:



Figure 13

218. Together, these network traffic requests show that Medallia does not just track anonymous web traffic, but actually intercepts the substance and content of users' Website Communications inside Defendants' purportedly secure portals. By enabling session replay in this way, Defendants allow Medallia to capture users' highly sensitive PHI and build profiles concerning individual users – an invasive and unlawful practice.

#### **D. Defendants' Enabling of Adobe's Tracking Technology on Defendants' Purportedly "Secure" Patient Portals**

##### **1. Adobe's Tracking Technologies**

219. Adobe is another Third-Party Vendor. Defendants have embedded Tracking Technologies that enable Adobe to harvest the private data of insureds

while logged in to their patient portals on Defendants' Website for marketing and commercial purposes, without adequately disclosing this fact to users or obtaining consent.

220. Adobe is a software company headquartered in San Jose, California. While known for its products like Photoshop and Acrobat, it also operates a number of digital marketing and data analytics tools used to track behavior across websites.

221. These data products include Adobe Analytics,<sup>62</sup> Adobe Experience Platform,<sup>63</sup> and Adobe Audience Manager,<sup>64</sup> all of which use Tracking Technologies like beacons, pixels, JavaScript tags, cookies, and session replay code to capture data in real time.

222. Defendants embedded Adobe's Tracking Technologies on the Website, including in insureds' purportedly "secure" patient portals.

223. Defendants' embedding of Adobe's code on the Website allowed Adobe to surreptitiously harvest data about insureds' visits, including keyword searches, and match these data to offline profiles.

224. Further, by embedding this tracking inside portals, Defendants violated HIPAA's privacy rules by improperly disclosing PHI to the Third-Party Vendors. This violation occurred even if Plaintiffs had not done a single search, as patient status itself is PHI under HIPAA, and Plaintiffs' logins confirmed that they

---

<sup>62</sup> *Adobe Analytics*, ADOBE FOR BUSINESS, <https://business.adobe.com/products/adobe-analytics.html> [<https://perma.cc/MX45-HTSE>].

<sup>63</sup> *Adobe Experience Manager*, ADOBE FOR BUSINESS, <https://business.adobe.com/products/experience-manager/sites/aem-sites.html> [<https://perma.cc/3X55-WWKT>].

<sup>64</sup> *Adobe Audience Manager*, ADOBE FOR BUSINESS, <https://business.adobe.com/products/audience-manager/adobe-audience-manager.html> [<https://perma.cc/C5DG-89MH>].

are receiving or have received care. *See Nienaber v. Overlake Hosp. Med. Ctr.*, 733 F. Supp. 3d 1072, 1081–82 (W.D. Wash. 2024) (stating, within a HIPAA framework, “[a]s other Courts within this Circuit have acknowledged, the transmission of information submitted to a *private patient portal*—such as a user clicking on the ‘log in’ button on that webpage—reveals patient status, which in and of itself is protected health information.”); *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 793 (N.D. Cal. 2022) (finding that “patient status is protected health information” under HIPAA).

## 2. Real-Time Transmission of Sensitive Health Data

225. The following code from Defendants’ Website shows how highly sensitive, private, personal data are intercepted by Adobe as an insured actively navigates their patient portal:

| ▼ General                   |                                                                                                                                 |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Request URL                 | <a href="https://assets.adobedtm.com/77d981f695af/ba740136c5b4/au">https://assets.adobedtm.com/77d981f695af/ba740136c5b4/au</a> |
| Request Method              | GET                                                                                                                             |
| Status Code                 | ● 200 OK (from disk cache)                                                                                                      |
| Remote Address              | 23.14.57.83:443                                                                                                                 |
| Referrer Policy             | no-referrer-when-downgrade                                                                                                      |
| ▼ Response Headers          |                                                                                                                                 |
| Accept-Ranges               | bytes                                                                                                                           |
| Access-Control-Allow-Origin | <a href="https://membersecure.anthem.com">https://membersecure.anthem.com</a>                                                   |
| Cache-Control               | max-age=3600                                                                                                                    |
| Content-Encoding            | gzip                                                                                                                            |
| Content-Length              | 440675                                                                                                                          |
| Content-Type                | <a href="#">application/x-javascript</a>                                                                                        |
| Date                        | Thu, 02 Oct 2025 15:33:46 GMT                                                                                                   |
| Etag                        | "4600bfa05519361f53437c652420ad28:1759171695.288275"                                                                            |
| Expires                     | Thu, 02 Oct 2025 16:33:46 GMT                                                                                                   |
| Last-Modified               | Mon, 29 Sep 2025 18:48:16 GMT                                                                                                   |
| Server                      | <a href="#">AkamaiNetStorage</a>                                                                                                |
| Timing-Allow-Origin         | *                                                                                                                               |
| Vary                        | Accept-Encoding                                                                                                                 |
| X-Content-Type-Options      | nosniff                                                                                                                         |

*Figure 14*

226. As shown in the above screenshot, Defendants' Website loads third-party tracking code from Adobe via another network traffic request to <https://assets.adobedtm.com>, a domain controlled by Adobe's Digital Tag Manager platform.

227. The request retrieves and executes a JavaScript file, called (application/x-javascript), from a third-party Adobe server hosted by AkamaiNetStorage, which serves as the primary content delivery network for Adobe.<sup>65</sup>

228. Once loaded, this script activates and manages trackers, such as session replay and marketing beacons, which form the basis of pages of code too detailed and complicated to reprint in their entirety here:

```

1 // For license information, see `https://assets.adobedtm.com/77d981
2 (function(){window._satellite=window._satellite||{};window._satelli
3 ;if("object"===("void 0"===s?"undefined":o(s)))return s.v}}function
4 getIframeHost:function(e){if("string"===typeof e){var a=e.split("/")
5 ;!g._getField(T)&&a.e.isTrackingServerPopulated()}&&(o=g.cookieRead("
6 },{name:"prop13",type:"value",value:"Coronavirus Resource Center -
7 value:"Anthem Public Portal"},{name:"prop12",type:"value",value:"Co
8 elementSelector:'[data-analytics="edi270271RealTimeLink"]',bubbleFi
9 value:"Anthem Public Portal"},{name:"prop12",type:"value",value:"In
10 modulePath:"adobe-analytics/src/lib/actions/sendBeacon.js",settings
11 name:"prop5",type:"value",value:"Anthem Public Portal"},{name:"prop
12 value:"Medicare Part D - Compare MediBlue Rx Part D Plans Link"},{n
13 name:"Coronavirus Resource Center - How Can We Help Dropdown - See
14 value:"Getting Better Care - Find a Facility Link"},{name:"prop55",
15 type:"value",value:"Find Care - Guests - Select a Plan/Network Drop
16 settings:{type:"link",linkName:"",linkType:"o"}},{modulePath:"adobe
17 modulePath:"adobe-analytics/src/lib/actions/sendBeacon.js",settings
18 props:[{name:"prop5",type:"value",value:"Anthem Public Portal"},{na
19 value:"Provider Interactive Care Reviewer - Watch the Behavioral He
20 name:"prop12",type:"value",value:"Find Care - Guests - Type of Plan
21 elementSelector:'a[data-analytics="ptDDrugShopPlansButtonMcPartD"]'
22 value:"Home Page - Medicaid and State Sponsored Programs - Californ
23 modulePath:"core/src/lib/events/click.js",settings:{elementSelector
24 modulePath:"adobe-analytics/src/lib/actions/sendBeacon.js",settings
25 modulePath:"core/src/lib/conditions/path.js",settings:{paths:[{valu
26 bubbleFireIfChildFired:!1},ruleOrder:50]},conditions:[{modulePath:"
27 value:"Anthem Public Portal"},{name:"prop11",type:"value",value:"Re
28 anchorDelay:100,elementSelector:'a[data-analytics="healthInsuranceP
29 actions:[{modulePath:"adobe-analytics/src/lib/actions/setVariables.
30 modulePath:"core/src/lib/events/click.js",settings:{elementSelector
31 value:"Medicare Turning 65 - Adding Medicare Coverage - Collapse Tr
32 value:"Employer Anthem Life Employers, Employees, Producers - Emplo

```

Figure 15

<sup>65</sup> *Adobe-Managed Hosts Overview*, ADOBE EXPERIENCE LEAGUE (Apr. 1, 2025), <https://experienceleague.adobe.com/en/docs/experience-platform/tags/publish/hosts/managed-by-adobe-host> [https://perma.cc/VXR5-QA8W].

229. The above screenshot shows the JavaScript code embedded on Defendants' Website with Adobe Analytics configured to monitor and record user interactions with specific health-related links and buttons. For example, the code sets tracking for links labeled "Getting Better Care – Find a Facility Link," "Coronavirus Resource Center," and other pages associated with mental health and obtaining treatment.

230. Adobe's sendBeacon.js is an Adobe "tracking beacon" that is embedded on webpages and that transmits data to third-party Adobe servers in real time, without user knowledge or consent. A tracking beacon is a piece of code embedded in a website that is often invisible to the user. This particular beacon sends data, including what links users clicked or what content they entered, to Adobe.

231. This setup enables Adobe to receive the full content of Website Communications between users and Defendants' Website. That includes sensitive health-related search queries, button clicks, and navigation activity that reveal the users' medical interests, insurance status, or treatments.

232. For instance, as shown in Figure 16 below, when a user searches for "hysterectomy" on the "Benefits" tab of the patient portal, <https://assets.adobetm.com> transmits information associated with the user's activity that contains the *full and exact* content of that search (i.e., "Shop Procedures2 – Total Hysterectomy –

Compare Providers Link”) to Adobe Alloy (i.e., “adobe-alloy/dist/lib/actions/sendEvent/index.js), also known as Adobe Experience Platform:<sup>66</sup>

```

actions: [{
  modulePath: "adobe-alloy/dist/lib/actions/sendEvent/index.js",
  settings: {
    xdm: "%uploadBtnAddCouponSliderCarelionWebSdk%",
    type: "web.webinteraction.linkClicks",
    instanceName: "alloy",
    edgeConfigOverrides: {
      development: {}
    }
  }
}], {
  id: "RL80c47701cfc6435a9d9ca600140aa73c",
  name: "Shop Procedures2 - Total Hysterectomy - Compare Care Providers Link",
  events: [{
    modulePath: "core/src/lib/events/click.js",
    settings: {
      elementSelector: '[data-analytics = "hysterectomyShopProcFindCare"]',
      bubbleFireIfParent: !0,
      bubbleFireIfChildFired: !0
    }
  }
}]

```

Figure 16

233. Similarly, when a user enters “Obstetrics/gynecology” in a search field on the “Find Care” tab of the patient portal, the *full and exact* content of that search is embedded in a URL and transmitted to Adobe via a network traffic request from smetrics.anthem.com, which is actually Adobe’s analytics collection server, as shown in Figure 17 below:

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Request URL     | https://smetrics.anthem.com/b/ss/wlpreimaglobalprod/1/JS-2.27.0-LEWM/s27344401164376?AQ8=1&ndh=1&pf=1&xt=1%2F9%2F2d=063328420712304268038730374035375324708&aamlh=9&ce=UTF-8&g=https%3A%2F%2Fmembersecure.anthem.com%2Fmember%2Cevent55&c5=Secure&v5=D%3Dc5&c8=c4fe4cfd-ec3e-4446-be42-de8211f0dfd68v8=c4fe4cfd-ec3e-4446-be42-de8211f0dfd68v12=-%20Predictive%20Search%20Menu&v12=D%3Dc12&c55=Find%20Care%20-%20Search%20Page%20-%20Predictive%20Search%20Mer5M002%7CL06515D002%7CL06515D001%7CL06515V001&v91=mo&v92=I06515&v93=scrbr&v94=WGS20&v95=lg&v97=27-64&v100=37ef41fbda&v200=063328420712304268038730374035375324708&pe=ink_o&xpev2=Obstetrics%2Fgynecology&cs=1920x1080&cc=24&gj=orgid=95CF659E533DE4C90A490D4D%40AdobeOrg&rt=82&AQE=1 |
| Request Method  | GET                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Status Code     | 200 OK                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Remote Address  | 63.140.36.210:443                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Referrer Policy | origin-when-cross-origin                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

Figure 17

<sup>66</sup> Web SDK Guide: Frequently Asked Questions, ADOBE EXPERIENCE LEAGUE (Oct. 31, 2023), <https://experienceleague.adobe.com/en/docs/experience-platform/edge/web-sdk-faq#https://perma.cc/SZD5-TM6X>.

234. Not only does the request include the user’s search queries (“Obstetrics” and “gynecology”), page location, and behavioral tracking parameters, but as shown in Figure 18 it also assigns multiple identifiers and tracking cookies, including tracking cookies labelled “s\_ecid” and “QuantumMetricSessionID,” which allow Adobe (and Quantum Metric) to link the user’s search for fertility care to a unique profile and monitor the user’s behavior across sessions and the Internet.

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cookie | s_ecid=MC MID%7C06332842071230426803873037403537532470; Q<br>kndctr_95CF659E533DE4C90A490D4D_Ado beOrg_identity=CiYwNjM;<br>TLTSID=6be33531-ce4e-4bbd-92bc-1a8af17e64d5; at_check=true; A<br>AMCV_95CF659E533DE4C90A490D4D%40Ado beOrg=179643557%7C<br>1760024013%7C7%7CMCAAMB-1760024013%7CRKhpRz8krg2tLO6p<br>1759426413s%7CNONE%7CMCAID%7CNONE%7CMCCIDH%7C-6641<br>ak_bmsc=7ACF24BA70B0EB1F4A1E80C5DF0BD763~0000000000000C<br>fxkm7OfB5otDRYDxiThkr0sD0apwvukFm4cyvdNwJQ00kD325wlHoLvc<br>47Y7J+ECCAdvMth8UDVAEoPGMz58G4zCXqotMQt4saNlvqVETkht8Tl<br>iniefZix8cemOOX/4eUt5Uhd13OhkOy/mz2MsHk2Xu0Se7xRJ7Jqzh91<br>QuantumMetricSessionID=2613aa4354426e3933f4751d8c2d7b0a; |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

*Figure 18*

235. By embedding Adobe’s Tracking Technologies into patient portals, Defendants enabled the interception and transmission of highly sensitive PHI for commercial gain, in direct violation of insureds’ reasonable expectations of privacy.

## **VII. Plaintiffs Did Not Consent to Defendants’ Interception, Harvesting, and Collection of Their Personal Health Data**

### **A. Defendants Repeatedly Stated That They Would Protect Plaintiffs’ Personal and Private Health Data**

236. Defendants’ Website represents that it offers a secure and confidential digital experience for accessing health insurance services and health information.

As it states:

# Anthem Privacy Policies

Your privacy is a priority to us, and we take great care to protect your information.

*Figure 19*<sup>67</sup>

237. This messaging (i.e., “we take great care to protect your information”) strongly and unequivocally conveys to Website users that Defendants do not exploit their personal health data – including data collected via the Website – for marketing purposes or transmit data to third parties without clear consent.

238. In the same section of the Website, labeled “Anthem Privacy Policies,” Defendants further affirm, as shown below, that “[o]ur policies prohibit the unlawful disclosure of PII, PHI, and/or PI”:

We are committed to safeguarding the PII, PHI, and/or PI we receive from our customers and members through the use of physical, technical, and administrative safeguards.

Our policies prohibit the unlawful disclosure of PII, PHI and/or PI. We share it externally only where federal and state law allows or requires it. It is our policy to limit the access, use and disclosure of this information to be in line with the job duties of our associates, as well as applicable law.

*Figure 20*<sup>68</sup>

239. This language conveys a commitment to the protection of private user data, particularly PHI-like information that is expressly subject to HIPAA and privacy laws and regulations.

---

<sup>67</sup> *Privacy Policies*, ANTHEM, <https://www.anthem.com/privacy> (last updated November 5, 2025) [<https://perma.cc/2ZRA-2Y9A>].

<sup>68</sup> *Id.*

240. On the same page of the Website, as shown below, Defendants even expressly state that they will not “sell, license or disclose personal information” to third parties except with user authorization, when “such disclosure is necessary,” or when “required or permitted by law.”

We may also gather quantitative user information, such as the number of users and the pages or data accessed, in order to perform administrative, technical, hosting or other functions that help us manage our website and application and deliver new functionality to you. We do not sell, license, transmit or disclose personal information that you provide to us to third parties except with the following exceptions:

- Upon your authorization;
- When such disclosure is necessary to allow us and our contractors or agents to carry out treatment, payment or healthcare operations; or
- When required or permitted by law.

*Figure 21*<sup>69</sup>

241. These representations led insureds to reasonably believe that Defendants do not share or disclose sensitive health-related information to third parties without *express* authorization.

---

<sup>69</sup> *Id.*

242. As shown below in Figure 22, additional representations accessible in the patient portal on a Website page titled “Laws and Rights that Protect You” further misled insureds to believe their health-related data were protected under ambiguously referenced “state and Federal laws:”

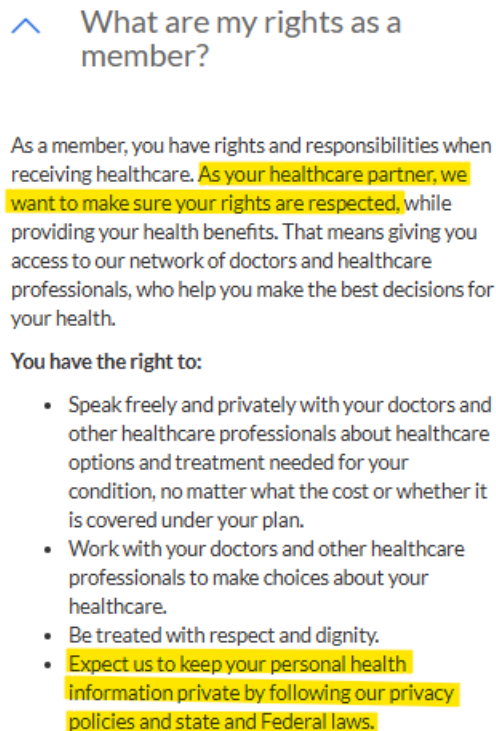


*Figure 22*

243. Here again, Defendants convey to Website users that Defendants are committed to respecting user rights, such as the privacy of personal health information, including through compliance with Website privacy policies such as those enumerated above in Figure 22.

## **B. Defendants’ Unlawful Interception of Plaintiffs’ Website Communications**

244. Tracking Technologies on Defendants’ Website, including Tracking Pixels and Session Replay Code, begin intercepting a user’s Website

Communications *immediately* upon the loading of Defendants' Website and the purportedly secure portals.

245. Defendants' Website does not display a pop-up, banner, or consent prompt when users begin interacting with coverage tools, provider searches, or other health-related features.

246. Defendants' Website does not present its privacy policy in any conspicuous or easily accessible location before the tracking and data collection begins.

247. Instead, the privacy policy is buried in the footer of the homepage in a section misleadingly entitled "Protecting Your Privacy," suggesting limited data collection, no surveillance or tracking, and no sharing of Plaintiffs' private health data with third parties.

248. Plaintiffs were not informed by Defendants that Tracking Technologies, including Tracking Pixels and Session Replay Code, were being used on Defendants' Website.

249. When a user navigates to Defendants' Website, the user is not presented with any notification or alert regarding the personal data collected by Tracking Technologies Defendants embedded in their Website.

250. Such notifications, which may be referred to as "pop-up" or "clickwrap" agreements, require a website user to affirmatively consent to their data being collected, often by selecting an option stating "I agree" or something similar.

251. Defendants' Website has not employed any such mechanisms that allow users to consent to the collection and dissemination of the private health data.

252. In contrast to a conspicuous pop-up or notification, the privacy policy on Defendants' Website is in a footer on the Website, requiring users to scroll to the very bottom of the Website, and is entitled "Protecting Your Privacy," as shown below in Figure 23:

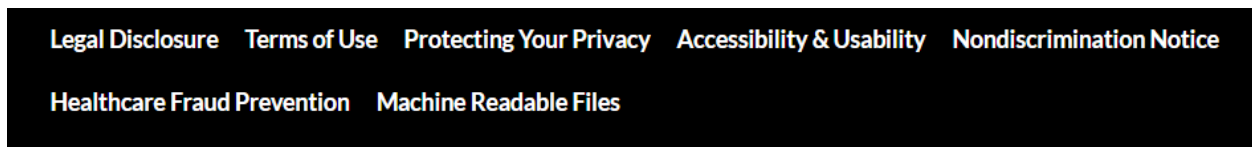


*Figure 23*<sup>70</sup>

253. The link to Defendants' privacy policies is presented in the same font size and color as the surrounding text, including non-hyperlinked text.

254. There is no language on Defendants' Website indicating the "Protecting Your Privacy" is (1) a hyperlink that (2) contains provisions that will bind the user.

255. Defendants' privacy policies further are never referenced in Defendants' "Terms of Use."

256. There is no language whatsoever in Defendants' terms of use informing users that, by simply using Defendants' Website, they are agreeing to Defendants' use of third-party Tracking Technologies and the real-time tracking and disclosure of their sensitive health-related information to Third-Party Vendors.

---

<sup>70</sup> *Main Page*, ANTHEM, <https://www.anthem.com/> [<https://perma.cc/56WP-5GBW>].

257. Further, Defendants' Terms of Use do not direct users to click on "Protecting Your Privacy" link or to read Defendants' privacy policies.

258. Once a Website user has located the "Protecting Your Privacy" link at the bottom of Defendants' Website and clicks on it, an image of a lock immediately loads before the written content:



*Figure 24*<sup>71</sup>

259. Users are presented with many options to click after the lock, including Introduction, Web Privacy Statement, and even a Privacy Authorization Form.

260. The third option, HIPAA Notice of Privacy Practices, opens a page with a link to a ten-page PDF that affirmatively states that the user's written permission is required for Defendants to use their PHI and gives the false impression that Tracking Technologies are not being used by Defendants, as shown below in Figure 25:

---

<sup>71</sup> *Privacy Policies*, ANTHEM, <https://www.anthem.com/privacy> [<https://perma.cc/2ZRA-2Y9A>].

**Sharing your PHI with others:** In most cases, if we use or share your PHI outside of treatment, payment, operations, or research activities, we have to get your approval in writing first. We must also get your written permission before:

- Using your PHI for certain marketing activities.
- Selling your PHI.
- Sharing any psychotherapy notes from your doctor or therapist.

*Figure 25*<sup>72</sup>

261. Later in the same PDF, Defendants once again reiterate that they will obtain written consent before sharing any PHI, as shown below in Figure 26:

**Authorization:** We'll get your written permission before we use or share your PHI for any purpose not stated in this notice. You may cancel your permission at any time, in writing. We will then stop using your PHI for that purpose. However, if we've already used or shared your PHI with your permission, we cannot undo any actions we took before you told us to stop.

*Figure 26*<sup>73</sup>

262. The PDF further purports to inform users about *all* of the ways in which their information or data or searches may be disclosed, as shown below in Figure 27:<sup>74</sup>

THIS NOTICE DESCRIBES HOW MEDICAL, VISION, AND DENTAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED, AND HOW YOU CAN GET ACCESS TO THIS INFORMATION WITH REGARD TO YOUR HEALTH BENEFITS. PLEASE READ CAREFULLY.

*Figure 27*

263. The fact that the relevant language above is capitalized implies that the content is important, and the “please read carefully” language strongly suggests

---

<sup>72</sup> *Notice of Privacy Practices*, ANTHEM, <https://www.anthem.com/content/dam/digital/docs/global/notices/privacy/privacy-practices-102256MUMENABS.pdf> [<https://perma.cc/Y5ED-LUZ6>].

<sup>73</sup> *Id.*

<sup>74</sup> *Id.*

to the user that Defendants have listed *all* of the ways in which their sensitive health information may be disclosed by Defendants.

264. If users close the PDF and return to Defendants' general subpage regarding privacy, they can scroll down and find a "Web Privacy Statement" that, as shown below, declares that privacy is "very important" to Defendants" and that they will "make every reasonable effort to safeguard" collected PHI, without explaining what information they collect, how they collect it, and how they safeguard it.

## Web Privacy Statement

Your privacy is very important to us, and we will make every reasonable effort to safeguard any information we collect.

This privacy statement is effective January 1, 2020, and was most recently reviewed in July 2024. This privacy statement is subject to change. We encourage you to review it from time to time.

### *Figure 28*<sup>75</sup>

265. It is only when users finally click on an additional dropdown menu under Defendants' "Web Privacy Statement" that "web trackers" are disclosed for the first time, in a general, non-specific manner that contradicts Defendants' other statements on the Website, as shown below in Figure 29:

---

<sup>75</sup> *Privacy Policies*, ANTHEM, <https://www.anthem.com/privacy> (last updated November 5, 2025) [<https://perma.cc/2ZRA-2Y9A>].

## What Information Will We Collect?



Information may be collected in the following ways on this website and application:

- If we provide user account access, you may elect to establish an account so that you can gain additional access to online service applications, health tools, health information, subscriptions, or other services where it is important for us to know who you are in order to best meet your needs. Providing personal information is always voluntary.
- We may use “cookies” and/or other web trackers to help us improve this website and application by tracking your navigation habits and to store some of your preferences. A cookie is a small file created by a website or application to store information on your computer. Cookies do not allow websites or applications to gain access to other information on your computer. Once a cookie is saved on your computer, generally only the website or application that created the cookie can read it.
- An Internet Protocol (IP) address is a number that automatically identifies the computer or mobile device that you are using to access the Internet. The IP address enables our server to send you the site pages that you want to visit or the data you want to view. The IP address may disclose the server owned by your Internet Service Provider. We use your IP address to help diagnose problems with our server and to support our administration of this website and application.

### *Figure 29*<sup>76</sup>

266. The “disclosures” above, which are buried in a lengthy paragraph with generic, boilerplate language, include vague and nonspecific phrasing like “we *may* use cookies” to “store some of your preferences.”<sup>77</sup>

267. The disclosures also fail to identify any specific Third-Party Vendors and refer only to “web trackers,” which users are not informed are *third-party* web trackers that send information to third parties without users’ consent.

268. The disclosures further fail to specify what types of data are collected, or that the Tracking Technologies may identify, profile, or link users across multiple sessions or even the Internet. The disclosures do not refer to Session Replay that records users’ entire sessions, including typed input, mouse movements, and navigations.

---

<sup>76</sup> *Id.*

<sup>77</sup> *Id.*

269. The disclosures fail to provide any opt out like a “reject” or “do not track” option.

270. The disclosures are not presented at the point of data collection, such as when a user begins typing a sensitive medical condition.

271. Remarkably, the disclosures *themselves* make heavy use of Tracking Technologies, with the Third-Party Vendors instantly tracking user’s clicks and what they review. For instance, when users click on the aforementioned HIPAA Notice of Privacy Practices, as shown in Figure 30 below Quantum Metric instantly collects this information through POST requests that send user data to Quantum Metric servers:

| ▼ General       |                                                                                                                                                                                                                                                         |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Request URL     | https://ingest.quantummetric.com/horizon/anthem?T=B&u=https%3A%2F%2Fwww.anthem.com%2Fprivacy%233&t=1754493000167&v=1754493000371&H=48709368d85c8c4486862447&s=d409cb802f294438bf6e0c93d653c18b&U=b677b9e7c0ae84ae1ef95b34c2ffb821&N=0&Q=2&S=0&b=570&z=1 |
| Request Method  | POST                                                                                                                                                                                                                                                    |
| Status Code     | ● 200 OK                                                                                                                                                                                                                                                |
| Remote Address  | 130.211.11.183:443                                                                                                                                                                                                                                      |
| Referrer Policy | strict-origin-when-cross-origin                                                                                                                                                                                                                         |

*Figure 30*

272. Users are not asked to consent prior to browsing Defendants’ Website, and they are wiretapped from the moment they load the site,<sup>78</sup> regardless of whether they eventually navigate to, download, read, or understand the disclosures in the privacy notice.

---

<sup>78</sup> *Javier v. Assur. IQ, LLC*, No. 21–16351, 2022 U.S. App. LEXIS 14951, at \*5 (9th Cir. May 31, 2022) (retroactive consent is not consent for digital wiretapping).

273. Defendants do not offer users any mechanism to meaningfully opt out of such data collection.

274. At no point do Defendants seek affirmative consent from users prior to the initiation of data tracking.

275. Valid consent to interception must be actual, informed, and voluntary.

276. In sum, the privacy policy on Defendants' Website is structured to deflect users' attention from Defendants' impermissible, unlawful collection of users' private data by publishing misleading general, non-specific disclosures spread across several subpages of the Website, some of which directly conflict with other purported disclosures. Defendants provide no explanation of the Tracking Technologies, no accurate or complete disclosure about the sharing of queries and sensitive information with third parties (including the names of the third parties with whom Defendants unlawfully share insureds' private information), and no way to opt out of the sharing of private information. Insureds like Plaintiffs, who reasonably expect confidentiality on a "personal" healthcare website, are left unaware that their keystrokes, searches, and clicks are being intercepted in real time. This deception cannot constitute actual, informed, or voluntary consent.

277. In light of the above, Plaintiffs did not consent to Defendants' interception and collection of their Website Communications.

**C. Defendants' Conduct Violates HIPAA's Privacy Rules**

278. Because Defendants' Website is branded with the name Anthem, a health insurance provider, users have an elevated expectation that their activity will remain private and secure.

279. Courts and regulators have recognized that health-related data warrants elevated privacy protections due to its sensitivity and the risk of its misuse.

280. HIPAA's enhanced protections for health-related data support the conclusion that Plaintiffs had a reasonable expectation of privacy in interacting with Defendants' Website.

281. HIPAA prohibits business associates of covered entities like Defendants from using or disclosing PHI for purposes such as marketing, analytics, or other transmissions to third parties, unless the individual has provided a valid, written authorization. *See* 45 C.F.R. § 164.508(a)(3).

282. A valid HIPAA authorization must be written, specific, and signed by the individual. It must identify the data to be used or disclosed, the recipient, and the purpose. *See* 45 C.F.R. § 164.508(c)(1)(i)–(vi).

283. Defendants' integration of tracking technologies on its pages results in the automatic and unauthorized transmission of sensitive health-related data of the insureds of Anthem to third parties that include the Third-Party Vendors.

284. At no point did Defendants obtain HIPAA-compliant written authorizations from such users before this transmission occurred.

285. The privacy policy on Defendants' Website does not provide the specificity, clarity, or accessibility required to satisfy HIPAA's notice and its authorization requirements.

286. Defendants' failure to transparently disclose its data practices, along with how users engage with the Defendants' Website, violates HIPAA's core principle that individuals must be given control over their health information and be empowered to authorize or reject such disclosures.

287. By covertly transmitting user interactions related to health services to third parties without authorization, Defendants have failed to meet the heightened duty of care owed to entities in possession of sensitive health information, as memorialized in HIPAA's statutory and regulatory regime.

288. Defendants failed in their core healthcare obligations by prioritizing marketing analytics and commercial gain over patient privacy.

**D. Tolling of the Statutes of Limitation**

289. None of the Plaintiffs were aware that their private health data were being intercepted and sent to the Third-Party Vendors.

290. None of the Plaintiffs consented to Defendants and the Third-Party Vendors intercepting their private health data.

291. Plaintiffs could not have, despite full diligence, discovered the full scope of Defendants' conduct as alleged herein, as there was no indication of the scope of the above-described tracking technologies that Defendants employ on Defendants' Website.

292. Accordingly, the applicable statutes of limitation have been tolled as a result of Defendants' knowing and active concealment and denial of the full scope of its use of these tracking technologies.

293. Defendants were under a duty to disclose the nature and extent of their data collection practices but did not do so.

294. Defendants are therefore estopped from relying on any statute of limitations defenses.

### **CLASS ACTION ALLEGATIONS**

295. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23, individually and on behalf of a putative class of the following similarly situated individuals (collectively, the “Class”):

Every current and former insured of Anthem whose Website Communications were captured, from November 6, 2023, through the date of the judgment, through the use of Tracking Pixels and/or Session Replay Code embedded in Defendants’ Website, [www.anthem.com](http://www.anthem.com), subpages, and patient portals to the date of judgment herein.

296. **Numerosity:** The Class includes thousands of people, such that it is not practicable to join all class members into one lawsuit.

297. **Commonality:** This case presents questions of law and fact that are common to the Class, including:

- Whether Defendants enable Third-Party Vendors to intercept the Website Communications of users to Defendants’ Website, [www.anthem.com](http://www.anthem.com), subpages, and insureds’ portals;
- Whether Defendants intentionally disclose the intercepted Website Communications of the Website users;

- Whether Defendants acquire the contents of Website users' Website Communications without their consent;
- Whether Defendants' conduct violates FWA and Indiana common law;
- Whether Plaintiffs and Class members are entitled to equitable relief; and
- Whether Plaintiffs and Class members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

298. **Typicality:** Plaintiffs, Class members, and Defendants have a commonality of interest in the subject matter of the lawsuit and the remedy sought.

299. **Predominance:** The common questions of law and fact predominate over any individual issue that may arise on behalf of an individual Class member.

300. **Superiority:** A class action is the appropriate vehicle for fair and efficient adjudication of the claims of Plaintiffs and Class members because if individual actions were required to be brought by each member of the Class, the result would be a multiplicity of actions, creating hardship to the Class, to the Court, and to Defendants.

301. **Adequacy of representation:** Plaintiffs and counsel will fairly and adequately protect the interests of Class members. Plaintiffs' counsel, Schlichter Bogard, will fairly and adequately represent the interests of the Class. Schlichter Bogard has a well-documented track record of successfully serving as class counsel in this Circuit and elsewhere. Schlichter Bogard's pioneering work in class actions

has been covered by numerous national publications, including the *New York Times* and *Wall Street Journal*, among other media outlets.

302. Schlichter Bogard has also been widely recognized by federal judges across the United States as pioneers in fiduciary breach class action litigation. Schlichter Bogard's vast experience in this area is reflected by the firm's appointment as class counsel in over 30 fiduciary breach class actions.

303. Federal judges have repeatedly recognized that Schlichter Bogard's efforts and successful outcomes have led to "enormous" savings for class members. *E.g., Cates v. Trs. of Columbia Univ.*, No. 1:16-cv-06524-GBD, 2021 U.S. Dist. LEXIS 200890, at \*15–16 (S.D.N.Y. Oct. 18, 2021).

304. Schlichter Bogard has additionally handled, and repeatedly prevailed in, fiduciary breach class action litigation in the U.S. Supreme Court. For example, in *Tibble v. Edison International*, a landmark fiduciary breach class action handled by Schlichter Bogard, after a partial loss in the U.S. District Court for the Central District of California, which was upheld by the U.S. Court of Appeals for the Ninth Circuit, Schlichter Bogard achieved a reversal before the Supreme Court of the United States. The Supreme Court's vacatur in favor of the plaintiffs was unanimous. *See Tibble v. Edison Int'l*, 135 S. Ct. 1823 (2015).

305. Schlichter Bogard secured a reversal of a dismissal before the U.S. Supreme Court, again in a unanimous decision, in *Hughes v. Northwestern University* – another fiduciary breach class action. *See Hughes v. Nw. Univ.*, 595 U.S. 170 (2022).

306. In *Cunningham v. Cornell University*, yet another fiduciary breach class action, which was decided by the U.S. Supreme Court this year, Schlichter Bogard again achieved a unanimous victory. *See Cunningham v. Cornell Univ.*, 604 U.S. 693, 695, 145 S. Ct. 1020, 1024 (2025).

307. Other courts have repeatedly heralded Schlichter Bogard's work in class action litigation. By way of limited example:

308. Judge Tanya Walton Pratt of this District recognized Schlichter Bogard's "extraordinary skill and determination" in securing a \$23.65 million monetary recovery and over \$62 million in total value for plan participants. *See Bell v. Pension Comm. of ATH Holding Co., LLC*, No. 15-2062-TWP-MPB (S.D. Ind. Sep. 4, 2019), Doc. No. 380. The court praised the firm for its role as "private attorney general risking large sums of money and investing thousands of hours for the benefit of employees and retirees." *Id.* at 3. Notably, only one objection was received from a class of over 127,000 members, which was a "remarkable sign of the Class's overwhelming support." *Id.* at 2.

309. Another U.S. district judge found as follows: "Class Counsel performed substantial work . . . investigating the facts, examining documents, and consulting and paying experts to determine whether it was viable. This case has been pending since September 11, 2006. Litigating the case required Class Counsel to be of the highest caliber and committed to the interests of the [class]." *Will v. General Dynamics*, No. 06-698, 2010 U.S. Dist. LEXIS 123349, at \*8–9 (S.D. Ill. Nov. 22, 2010).

310. Other findings by U.S. district judges in relation to Schlichter Bogard's work include the following: "Schlichter, Bogard & Denton has achieved unparalleled results on behalf of its clients, . . . has invested . . . massive resources and persevered in the face of . . . enormous risks[.]" *Nolte v. Cigna*, No. 07-2046, 2013 U.S. Dist. LEXIS 184622, at \*8 (C.D. Ill. Oct. 15, 2013) (obtaining recovery of \$35 million on behalf of plan participants in Cigna's 401(k) plan).

311. "Litigating this case against formidable defendants and their sophisticated attorneys required Class Counsel to demonstrate extraordinary skill and determination." *Beesley v. Int'l Paper Co.*, No. 06-703, 2014 U.S. Dist. LEXIS 12037, at \*8 (S.D. Ill. Jan. 31, 2014).

312. "Schlichter, Bogard & Denton demonstrated extraordinary skill and determination in obtaining this result for the Class." *Abbott v. Lockheed Martin Corp.*, No. 06-701, 2015 U.S. Dist. LEXIS 93206, at \*9 (S.D. Ill. July 17, 2015).

### **CAUSES OF ACTION**

#### **COUNT I – VIOLATION OF FEDERAL WIRETAP ACT (ON BEHALF OF PLAINTIFFS AND THE CLASS)**

313. Plaintiffs incorporate the preceding paragraphs as though fully realleged herein.

314. The FWA gives a private right of action to anyone whose communications are intercepted, disclosed, or used in violation of the statute. 18 U.S.C. § 2520(a).

315. The FWA, as amended by the ECPA, prohibits any person from intentionally intercepting, disclosing, or using the contents of any wire, oral, or electronic communication without consent or as otherwise permitted by law.

316. The FWA, as amended by the ECPA, extended wiretap protections to digital transmissions that those alleged herein.

317. Plaintiffs' interactions and Website Communications with Defendants' Website are "electronic communications" under 18 U.S.C. § 2510(12), and the information they contain constitutes "contents" under 18 U.S.C. § 2510(8).

318. Defendants, through tracking code embedded in their Website, intentionally intercepted these Website Communications and they were disclosed to the Third-Party Vendors without Plaintiffs' knowledge or valid consent.

319. Any alleged one-party consent by Defendants is invalid because Defendants committed a federal crime of "knowingly" disclosing "individually identifiable health information" to third parties. 42 U.S.C. § 1320d-6(a).

320. Any alleged one-party consent by Defendants is invalid because Defendants committed torts as outlined herein like intrusion upon seclusion.

321. As a result, the consent exception is void under the FWA and Defendants are liable for damages. 18 U.S.C. § 2511(2)(d).

322. Defendants are also liable under the FWA's prohibition on "procurement." 18 U.S.C. § 2511(1)(a). A party who procures another to intercept communications is equally liable as if it had conducted the interception by itself. *Id.*

323. Defendants knowingly embedded the Tracking Technologies of the Third-Party Vendors to allow them to capture Plaintiffs' Website Communications in real time, thereby "procuring" unlawful interceptions.

324. Defendants are further liable under the FWA because they used and disclosed the unlawfully intercepted contents of Plaintiffs' Website Communications, knowingly benefiting from this data by analyzing user behavior and targeting insureds for commercial purposes. 18 U.S.C. § 2511(1)(c)–(d).

325. Plaintiffs request the relief set forth in the Request for Relief below.

**COUNT II – BREACH OF FIDUCIARY DUTY**  
**(ON BEHALF OF PLAINTIFFS AND THE CLASS)**

326. Plaintiffs incorporate the preceding paragraphs as though fully realleged herein.

327. As covered entities under HIPAA, Defendants had a fiduciary duty to maintain the confidentiality and privacy of Plaintiffs' personal health information, including the Website Communications made on Defendants' Website.<sup>79</sup>

328. Concurrently, as a business associate of a covered entity under HIPAA, Elevance had a fiduciary duty to maintain the confidentiality and privacy of Plaintiffs' personal health information, including the Website Communications made on Defendants' Website.<sup>80</sup>

---

<sup>79</sup> 45 C.F.R. § 164.502 (uses and disclosures of PHI); *Walgreen Co. v. Hinchey*, 21 N.E.3d 99 (Ind. Ct. App. 2014) (upholding verdict against pharmacy employee and Walgreen's for unauthorized disclosure of PHI and mentioning HIPAA and other medical privacy statutes as guide).

<sup>80</sup> 45 C.F.R. § 164.502 (uses and disclosures of PHI).

329. Defendants likewise had a fiduciary duty, under Indiana law, to ensure the confidentiality of patient data, including § 16-39-5-3(f)–(h), 410 IAC 1-2.5-78, and Indiana Code § 16-39-2-6, which mandate that medical records and patient data be treated as confidential and subjects violators to criminal penalties.

330. Additionally, the Indiana Supreme Court has acknowledged that insured-insurer relationships can be fiduciary in nature.<sup>81</sup>

331. Defendants' fiduciary duty extended to ensuring that any collection, use, or sharing of personal health information was done only with the specific informed consent of the individual from whom the information was collected.<sup>82</sup>

332. At all relevant times, a relationship existed between Plaintiffs and Defendants, in which Plaintiffs entrusted Defendants to protect the private and personal health information of Plaintiffs and members of the putative class, and Defendants accepted that trust.

333. Defendants breached the fiduciary duty that it owed to Plaintiffs and the putative class by failing to act with the utmost good faith, fairness, and honesty; failing to act with the highest and finest loyalty; and failing to protect, or intentionally disclosing, this private and personal health information, while deliberately concealing their breaches from Plaintiffs.

334. Defendants' actions in enabling the interception and transmission of Plaintiffs' sensitive health information without informed consent constitutes a breach of the fiduciary duty that Defendants owe Plaintiffs under Indiana law.

---

<sup>81</sup> *Erie Ins. Co. v. Hickman*, 622 N.E.2d 515, 518–19 (Ind. 1993).

<sup>82</sup> *Id.*

335. As a direct result of Defendants' unauthorized disclosure of Plaintiffs' sensitive health information to Third-Party Vendors, Plaintiffs have suffered harm, including but not limited to the unauthorized disclosure of their highly sensitive health information, the risk of identity theft, and other potential damage arising from the unauthorized collection and sharing of personal health data.

336. Plaintiffs request the relief set forth in the Request for Relief below.

**COUNT III – INTRUSION UPON SECLUSION**  
**(ON BEHALF OF PLAINTIFFS AND THE CLASS)**

337. Plaintiffs incorporate the preceding paragraphs as though fully realleged herein.

338. Under Indiana law, the tort of intrusion upon seclusion occurs when a party intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or their private affairs, and the intrusion would be highly offensive to a reasonable person.<sup>83</sup>

339. Plaintiffs had a reasonable expectation of privacy in their interactions with Defendants' Website,<sup>84</sup> including in their search queries and page visits relating to their personal conditions and potential treatments.

340. Because Defendants' portals required login with usernames and passwords and represented themselves as secure healthcare tools, Plaintiffs' expectation of privacy was strong.

---

<sup>83</sup> *Cullison v. Medley*, 570 N.E.2d 27, 31 (Ind. 1991) (recognizing intrusion into "solitude or seclusion"); *Watters v. Dinn*, 633 N.E.2d 280, 290 (Ind. Ct. App. 1994) (either to his person or "to his private affairs or concerns").

<sup>84</sup> *Van Jelgerhuis v. Mercury Fin. Co.*, 940 F. Supp. 1344, 1368–69 (S.D. Ind. 1996) (comments in work environment about personal relationships of plaintiff constituted intrusion into "private affairs" and summary judgment denied).

341. Defendants' Website purports to offer security for accessing such health information.

342. However, without Plaintiffs' knowledge or consent, Defendants embedded Tracking Technologies (including those from the Third-Party Vendors) in the Website to record and transmit Website Communications in real time.

343. Defendants deliberately intruded into Plaintiffs' private affairs, in a way that a reasonable person would find highly offensive, especially given that the Defendants failed to disclose the extent of the Tracking Technologies and even made representations that users' information would remain confidential.

344. The conduct of Defendants involved the most private domain of all: Plaintiffs' health-related decisions and conditions inside a purportedly secure portal.

345. The offensive nature of the intrusion is heightened by the sensitivity of the subject matter, which Indiana statutes explicitly protect as confidential. *See, e.g.,* Ind. Code § 16-39-2-6 (confidentiality of mental health records); 410 IAC 1-2.5-78 (criminal penalties for improper disclosure of medical information).

346. In so doing, Defendants egregiously violated Indiana's privacy norms and legal protections.

347. As a direct and proximate result of Defendants' actions, Plaintiffs suffered and continue to suffer injuries, including loss of privacy, exposure to increased risk of identity theft, and loss of control over their private data.

348. Plaintiffs request the relief set forth in the Request for Relief below.

**COUNT IV – UNJUST ENRICHMENT**  
**(ON BEHALF OF PLAINTIFFS AND THE CLASS)**

349. Plaintiffs incorporate the preceding paragraphs as though fully realleged herein.

350. Under Indiana law, unjust enrichment occurs when a benefit was conferred upon Defendants, Plaintiffs conferred that benefit without compensation, and it would be inequitable for Defendants to retain that benefit without paying for its value.

351. Defendants obtained a significant financial benefit by covertly collecting, using, and sharing the personal health-related data of Plaintiffs with third parties, including the Third-Party Vendors, without consent.

352. Plaintiffs conferred a benefit – the use of their valuable personal health-related data – upon Defendants.

353. Defendants used Plaintiffs' valuable, personal health data for profit without Plaintiffs' authorization or consent.

354. Defendants have been unjustly enriched by using this sensitive health information, which has enormous value, to generate profits through targeted advertising and the sale or use of the data by third parties, including the Third-Party Vendors.

355. By collecting and transmitting these data without providing adequate notice or obtaining informed consent, Defendants have exploited the private health information of Plaintiffs for illicit financial gain, in violation of principles of fairness and equity.

356. Plaintiffs have suffered additional harm, including the loss of privacy and the potential for identity theft.

357. Defendants' conduct is inequitable because it is unfair for a business associate of a covered entity, who owes a fiduciary duty to protect the privacy and confidentiality of patients' health data, to harvest and profit from that information without consent.

358. The benefits that Defendants derived from Plaintiffs rightly belong to Plaintiffs as it is their private health information.

359. It would be inequitable under unjust enrichment principles for Defendants to retain any of the profits or other benefits derived from the practices alleged in this Complaint.

360. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs all unlawful or inequitable proceeds received as a result of the conduct alleged in this Complaint.

### **REQUEST FOR RELIEF**

Plaintiffs, on behalf of themselves and the Class, request judgment against Defendants as follows:

- A. Certifying this case as a class action, appointing Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class counsel for the Class;
- B. Finding that Defendants' conduct violates the FWA and Indiana Common Law;

- C. Awarding actual damages caused by Defendants' violations of FWA and Indiana Common Law;
- D. Awarding statutory damages as provided under 18 U.S.C. § 2520, including the greater of \$10,000 or \$100 per day for each violation of the FWA;
- E. Awarding compensatory damages, restitution, disgorgement, attorneys' fees and costs, and/or punitive damages as permitted by law and as the Court deems just and proper;
- F. Entering equitable relief enjoining Defendants from engaging in the misuse and/or disclosure of Plaintiffs' and Class members' data, and the issuance of prompt, complete and accurate disclosures to Plaintiffs, Class members, and all current and future users of the Website;
- G. Entering equitable relief requiring restitution and disgorgement of any profits wrongfully obtained as a result of Defendants' wrongful conduct;
- H. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable; and
- I. Awarding such other and further relief as this Court deems appropriate and as equity and justice may require.

**DEMAND FOR JURY TRIAL**

Plaintiffs, on behalf of themselves and the Class, request trial by jury of all claims asserted herein.

February 27, 2026

Respectfully submitted,

/s/ Andrew D. Schlichter

Andrew D. Schlichter\*

Alexander L. Braitberg\*

Chen Kasher\*

Cort VanOstran\*

SCHLICHTER BOGARD LLC

100 South Fourth Street, Suite 1200

St. Louis, MO 63102

(314) 621-6115

(314) 621-5934 (fax)

aschlichter@uselaws.com

abraitberg@uselaws.com

ckasher@uselaws.com

cvanostran@uselaws.com

Zoe Seaman-Grant\*

SCHLICHTER BOGARD LLC

33 North Dearborn Street, Suite 1170

Chicago, IL 60602

(919) 630-9301

zseamangrant@uselaws.com

\*Admitted *pro hac vice*

*Attorneys for Plaintiffs*

**CERTIFICATE OF SERVICE**

I hereby certify that on the 27th day of February 2026, a true and correct copy of the foregoing document was filed via the Court's CM/ECF filing system.

/s/ Andrew D. Schlichter  
Andrew D. Schlichter