

IN THE COURT OF COMMON PLEAS  
CUYAHOGA COUNTY, OHIO

JANE DOE, on behalf of herself and all others  
similarly situated  
c/o Spangenberg Shibley & Liber LLP  
1001 Lakeside Avenue East, Suite 1700  
Cleveland, OH 44114

Plaintiff

vs.

UNIVERSITY HOSPITALS HEALTH  
SYSTEM, INC.  
c/o ACFB Incorporated, Statutory Agent  
200 Public Square, Suite 2300  
Cleveland, OH 44114

Defendant

CASE NO.

JUDGE

**CLASS ACTION**

**JURY TRIAL DEMANDED**

**CLASS ACTION COMPLAINT**

Plaintiff, Jane Doe (“Plaintiff”), on behalf of herself and all others similarly situated, alleges as follows upon personal knowledge as to her own conduct and on information and belief as to all other matters based upon investigation by counsel, such that each allegation has evidentiary support or is likely to have evidentiary support upon further investigation and discovery.

**NATURE OF THE ACTION**

1. Plaintiff is a patient of Defendant University Hospitals Health System, Inc. (“UH”).
2. As Plaintiff’s health care provider, UH is prohibited from disclosing her personally identifiable, non-public medical information – including the content of her communications with UH – to third parties without her knowledge, consent, or authorization.



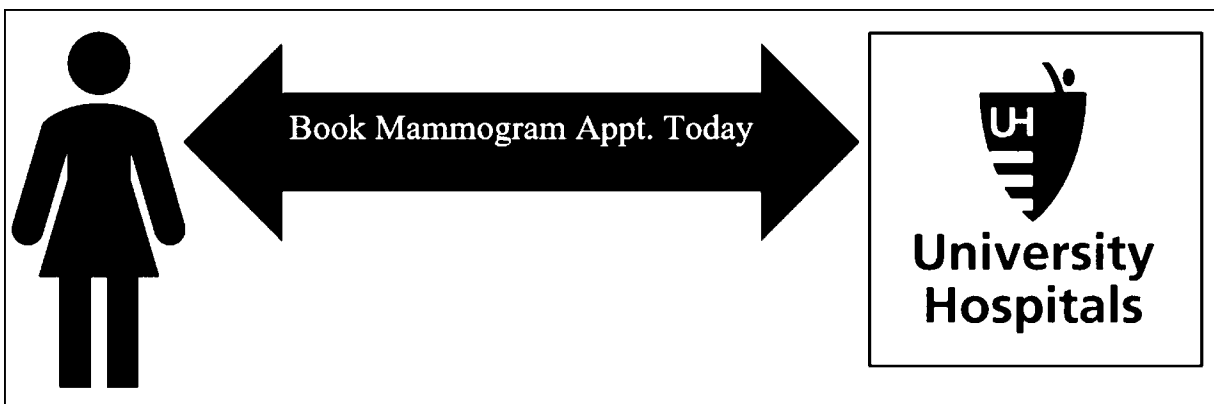
3. UH has a duty to its patients to keep their communications, diagnoses, and treatment completely confidential.

4. UH maintains a web property at [www.uhhospitals.org](http://www.uhhospitals.org) and an online patient portal through which it encourages patients to exchange communications to search for a doctor, learn more about their conditions and treatments, access medical records and test results, and make appointments.

5. UH expressly and impliedly promises Plaintiff and its patients that UH will maintain the privacy and confidentiality of communications that patients exchange with UH at its web properties.

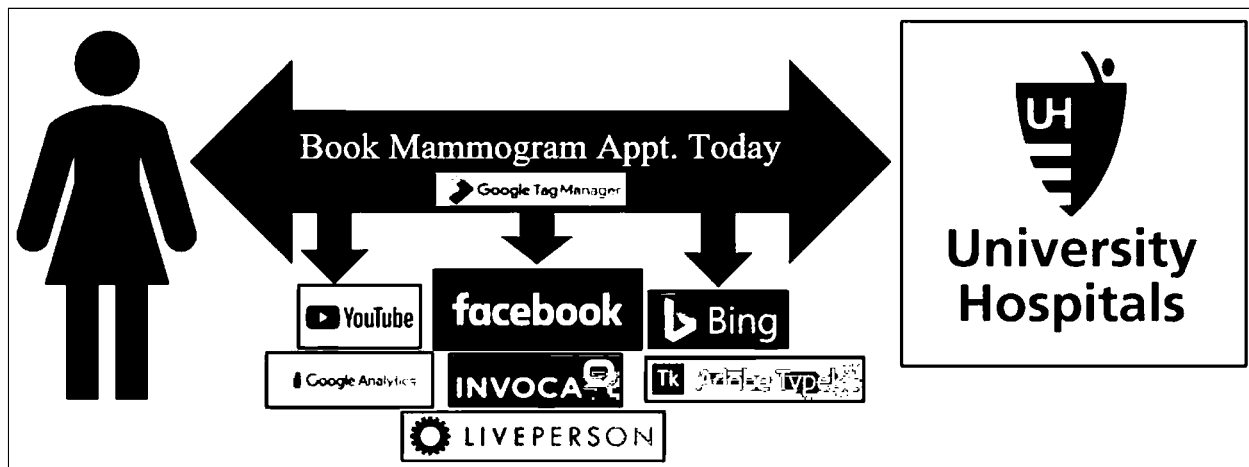
6. Based on patients' reasonable expectations of privacy, UH's express and implied promises, statutes, rules, and industry standards protecting patients' personally identifiable, non-public medical information, and communications, patients expect that communications exchanged with UH are between the patient and UH only and not shared with third parties.

7. A patient's reasonable expectations for communications with UH are illustrated as follows:





8. Instead, when a patient interacts with UH through its web properties, UH discloses the patient's personally identifiable, non-public medical information, and the contents of their communication to numerous third parties, illustrated as follows:



9. UH does not inform its patients that it makes these unauthorized, unprivileged disclosures of personally identifiable, non-public medical information to any of these third parties.

10. UH causes the unprivileged, unauthorized transmissions of personally identifiable, non-public medical information, and communications through computer source code that it deploys to command patient computing devices to transmit the data to third parties through invisible web bugs that include, but are not limited to, Facebook, Google, Microsoft (Bing), Invoca.net, Liveperson.net, LPSNMedia.net, and Typekit.net.

11. UH's conduct violates the common law and privacy laws of the State of Ohio

#### **PARTIES TO THE ACTION**

12. Plaintiff Jane Doe is an individual residing in Cuyahoga County, Ohio, a patient of Defendant University Hospitals, and user of the University Hospitals patient portal located at [www.uhhospitals.org](http://www.uhhospitals.org).



13. Defendant University Hospitals is a non-profit corporation organized and existing under the laws of Ohio with its headquarters at 3605 Warrensville Center Road, Shaker Heights, OH 44122.

14. Defendant University Hospitals is a covered entity under both Ohio Rev. Code § 3798.04 and the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d and 45 C.F.R. Part 160-45 C.F.R. Part 162, and 45 C.F.R. Part 164 “HIPAA”).

### **JURISDICTION AND VENUE**

15. This Court has jurisdiction pursuant to Ohio Revised Code Section 2305.01.

16. Venue is proper in Cuyahoga County pursuant to Ohio R.Civ.P. 3(C).

### **FACTS COMMON TO ALL COUNTS**

#### **STANDARDS FOR UH’S DUTY OF CONFIDENTIALITY AND AUTHORIZATION FOR DISCLOSURE OF MEDICAL INFORMATION**

##### ***Federal Law***

17. Under federal law, a health care provider may not disclose personally identifiable, non-public medical information about a patient, potential patient, or household member of a patient for marketing purposes without the patient’s express written authorization. *See* HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.501; 164.508(a)(3), 164.514(b)(2)(i).

18. Guidance from the United States Department of Health and Human Services instructs health care providers that patient status alone is protected by HIPAA.

19. In *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule*, the Department instructs:

Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a



phone book, then this information would not be PHI because it is not related to health data. ... If such information was listed with health condition, health care provision or payment data, *such as an indication that the individual was treated at a certain clinic*, then this information would be PHI. Emphasis added.<sup>1</sup>

20. In its guidance for Marketing, the Department further instructs:

The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. ... Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*. Emphasis added.<sup>2</sup>

### ***Ohio Law***

21. Ohio Rev. Code § 3798.04 similarly declares that a covered entity, such as a hospital, shall not "use or disclose protected health information without an authorization that is valid under 45 C.F.R. 164.508 and, if applicable, 42 C.F.R. part 2, except when the use or disclosure is required or permitted without such authorization by Subchapter C of Subtitle A of Title 45 of the Code of Federal Regulations and, if applicable, 42 C.F.R., part 2."

22. The Ohio Supreme Court has recognized that medical providers' duties of confidentiality and "an independent tort exists for the unauthorized, unprivileged disclosure to a third party of nonpublic medical information that a physician or hospital has learned with a physician-patient relationship." *Biddle v. Warren Gen. Hosp.*, 86 Ohio St. 3d 395, 401 (Ohio 1999).

### ***Ancient and Modern Industry Standards of Patient Confidentiality***

23. A medical provider's duty of confidentiality to his or her patients is ancient.

---

<sup>1</sup>[https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs\\_deid\\_guidance.pdf](https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf) at 5.

<sup>2</sup><https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf> at 1-2.



24. The original Hippocratic Oath, circa 400 B.C., provided that physicians must pledge, “Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not be spoken of outside, I will keep secret, as considering all such things to be private.”<sup>3</sup>

25. The modern Hippocratic Oath provides, “I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know.”

26. A medical provider’s duty of confidentiality to patients still applies today. In fact, the American Medical Association’s (“AMA”) Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

27. AMA Code of Medical Ethics Opinion 3.1.1 provides:

Protecting information gathered in association with the care of the patient is a core value in health care. However, respecting patient privacy in other forms is also fundamental, as an expression of respect for patient autonomy and a prerequisite for trust. Patient privacy encompasses a number of aspects, including ... personal data (informational privacy)[.] ... *Physicians must seek to protect patient privacy in all settings to the greatest extent possible* and should: (a) Minimize intrusion on privacy when the patient’s privacy must be balanced against other factors. (b) Inform the patient when there has been a significant infringement on privacy of which the patient would otherwise not be aware. [and] (c) Be mindful that individual patients may have special concerns about privacy in any or all of these areas. (emphasis added).

28. AMA Code of Medical Ethics Opinion 3.2.4 provides:

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

---

<sup>3</sup> Translation of Original Hippocratic Oath by Michael North, National Library of Medicine, National Institutes of Health, [https://www.nlm.nih.gov/hmd/greek/greek\\_oath.html](https://www.nlm.nih.gov/hmd/greek/greek_oath.html)



surrogate when the individual lacks decision-making capacity) about the purpose(s) for which access would be granted. (emphasis added).

29. AMA Code of Medical Ethics Opinion 3.3.2 provides:

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

### ***Patient Expectations of Patient Privacy***

30. Confidentiality is a cardinal rule of the provider-patient relationship.

31. Patients are aware of their medical provider's duty of confidentiality, and, as a result, have objectively reasonable expectations that their health care providers will not share their personally identifiable, non-public medical information, and communications with third parties in the absence of authorization for any purpose that is not directly related or beneficial to patient care.

32. A recent national survey from CVS-Aetna revealed that "[p]rivacy and data security lead patients' concerns in the changing health environment." 80 percent of survey respondents "indicated that privacy was a top concern regarding their health care, while 76 percent of individuals felt the same high level of concern for their data security." Both totals are higher than the 73 percent of consumers who indicated that cost is important to their care.

### ***UH's Express and Implied Promises of Confidentiality***

33. UH maintains its [www.uhhospitals.org](http://www.uhhospitals.org) property and its patient portal with knowledge that the property is used by patients to exchange communications with UH relating to their providers, treatments, services, and access to a promised "secure" patient portal called MyUHCare.



34. UH does not inform patients that their personally identifiable information and the content of their communications at [www.uhhospitals.org](http://www.uhhospitals.org) and MyUHCare are disclosed to Facebook, Google, and numerous other third parties for marketing purposes.

35. UH does not obtain any authorization from patients to use their data and communications at [www.uhhospitals.org](http://www.uhhospitals.org) for marketing purposes in connection with third parties.

36. Instead of providing notice and obtaining authorization for use of patient data and communications for marketing purposes, UH expressly promises confidentiality.

37. The [www.uhhospitals.org](http://www.uhhospitals.org) property includes two separate privacy statements:

- a. A “HIPAA Notice of Privacy Practices”; and
- b. A “Privacy Policy.”

38. As discussed in more detail below, UH makes numerous false or misleading statements about privacy in these documents.

**HOW UH DESIGNED ITS WEBSITE TO SECRETLY DISCLOSE PERSONALLY IDENTIFIABLE,  
NON-PUBLIC MEDICAL INFORMATION TO THIRD PARTIES**

***UH’s Web Property***

39. Defendant maintains a website designed for patients to communicate with Defendant, including, but not limited to, exchanging communications about conditions, treatments, providers, payments, and access to medical records through the MyUHCare patient portal.

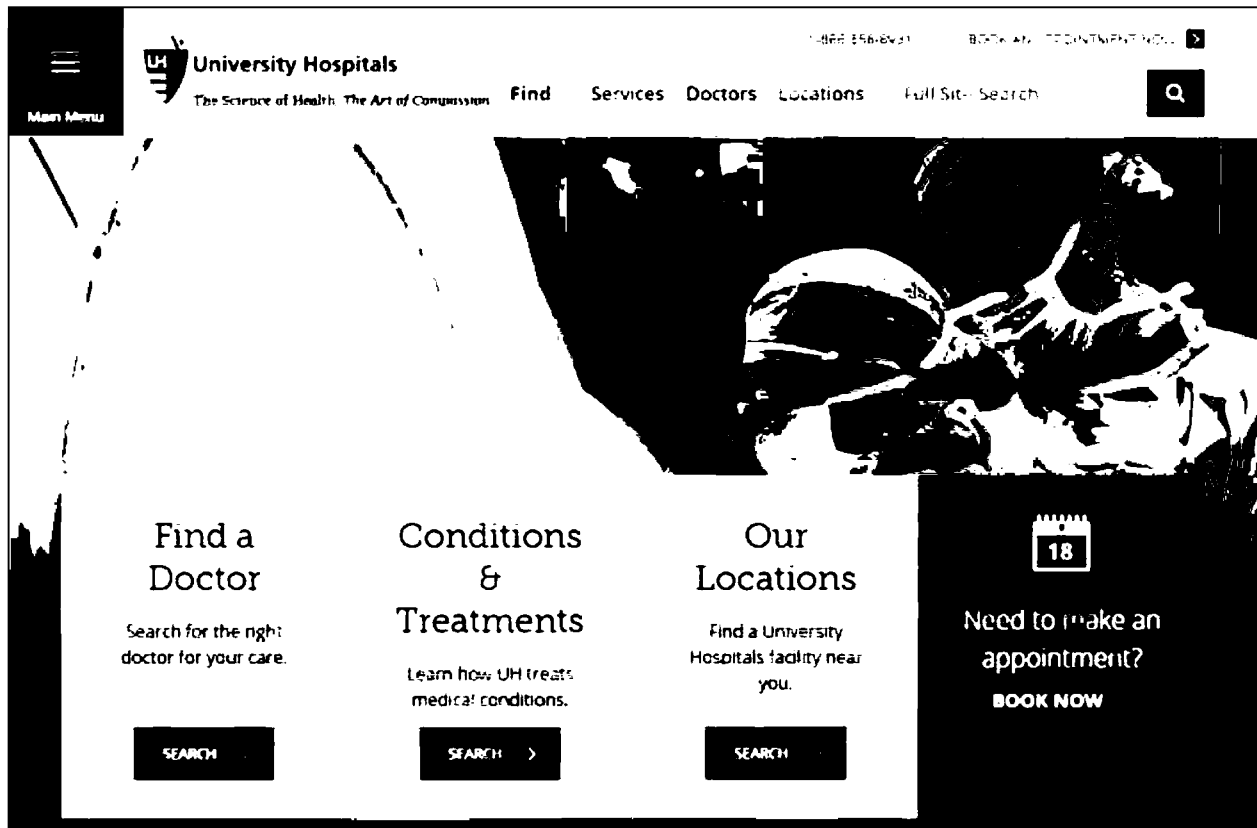
40. Defendant actively encourages patients to use the [www.uhhospitals.org](http://www.uhhospitals.org) website.

41. Defendant’s home page at [www.uhhospitals.org](http://www.uhhospitals.org) shows how the website is designed for use by Defendant’s patients and potential patients. The home page provides patients with prominent links to, among other things:

- a. Find a Doctor – Search for the right doctor for your care;



- b. Conditions & Treatments – Learn how UH treats medical conditions;
- c. Our Locations – Find a University Hospitals facility near you.
- d. Need to make an appointment? BOOK NOW; and
- e. Book an Appointment Now:



### *Basic Concepts of Webpage Design and Operation*

#### **Source Code**

42. Web browsers are software applications that allow consumers to exchange electronic communications over the Internet.

43. Every website is hosted by a computer server through which the entity in charge of the website exchanges communications with Internet users via their web browsers.

44. The basic command that web browsers use to communicate with website servers is called a GET request. For example, when a patient types



<https://www.uhhospitals.org/services/cancer-services/breast-cancer/breast-cancer-in-women> into the navigation bar of his or her web browser (or, just as frequently, takes the technological shortcut of clicking a hyperlink), the patient's web browser makes connection with the server for UH and sends the following request: "GET/services/cancer-services/breast-cancer/breast-cancer-in-women HTTP/1.1".

45. The other basic request utilized by web browsers is a POST request, which is typically employed when a user enters data into a form on a website and clicks 'Enter' or a submit button. 'POST' sends the data entered in the form to the server for the website.

46. In response to receiving a GET or POST request, the server for the entity with which the user is exchanging communications will send a set of instructions to the web browser, commanding the browser with source code that directs the browser (1) how to render the website's response communication and, in many circumstances, (2) commands the browser to contemporaneously re-direct the precise content of the user's communications to third parties.

47. The set of instructions that command the browser is called source code.

48. Source code may also command a web-browser to send data transmissions to third parties via pixels or web bugs, tiny 1x1 invisible GIF files that effectively open a spying window through which a website funnels data about users and their actions to third parties.

49. The third parties to whom a website transmits data through pixels or web bugs do not provide any substantive content relating to the user's communication. Instead, these third parties are typically procured to track user data and communications for marketing purposes.

50. The web bugs are tiny and camouflaged to purposefully remain invisible to the user.

51. Thus, without any knowledge, authorization, or action by a user, a website developer like UH's can use its source code to commandeer the user's computing device, causing



the device to contemporaneously and invisibly re-direct the user's personally identifiable, non-public medical information to third parties.

### **Tag Managers**

52. Web bugs or web pixels can either be placed directly on a page by a web developer or funneled through a "tag manager" service to make the invisible tracking more efficient and further obscure the third parties to whom user personally identifiable, non-public information, and communications are re-directed without their knowledge, consent, or any further action.

53. In the absence of a tag manager, a website developer who chooses to deploy third party source code on their website must enter the third-party source code directly onto their website for every third party to whom they wish to direct user data and communications. On websites with several third-party trackers, this may cause the page to load more slowly and increases the risk of a coding error effecting functionality and usability. A "tag manager" offers the website developer a solution. Instead of placing all third-party source code directly on the webpage, the developer places the source code for the tag manager. The developer then places the other third-party source code within its account at the tag manager.

54. Google explains the benefits of Google Tag Manager in an Introduction to Google Tag Manager video on YouTube.<sup>4</sup> Google explains:

Tags on your website help you measure traffic and optimize your online marketing. But all that code is cumbersome to manage. It often takes too long to get new tags on your site or update existing ones. This can delay campaigns by weeks or months so you miss valuable opportunities, data, and sales. That's where tag management comes in. Google Tag Manager is a powerful free tool that puts you the marketer back in control of your digital marketing. You update all your tags from Google Tag Manager instead of editing the site code. This reduces errors, frees you from having to involve a web master, and lets you quickly deploy tags on your site.

---

<sup>4</sup> See <https://www.youtube.com/watch?v=KRvbfPeZ11Y>, audio from 0:04 to 1:40.



Here's how it works. Sign in with an existing Google Account. Go to Google.com/tagmanager and create an account for your company. We'll name this one after the name of our company, Example Inc. Next, create a container for your domain name. We'll name this one after our website, example.com. This container will hold all the tags on the site. When you create a container, Google Tag Manager generates a container snippet to add to your site. Copy this container snippet and paste it into every page of your site. Paste the snippet below the opening body tag. Once you've pasted the container snippet into your site, you add and edit your tags using Google Tag Manager. You can add any marketing or measurement tag you want, whenever you want.

55. UH deploys Google Tag Manager on its websites through an "iframe," a nested "frame" that exists within the UH website that is, in reality, an invisible window through which UH funnels web bugs to secretly transmit personally identifiable, non-public medical information to third-parties without any knowledge, consent, authorization, or further action of patients.

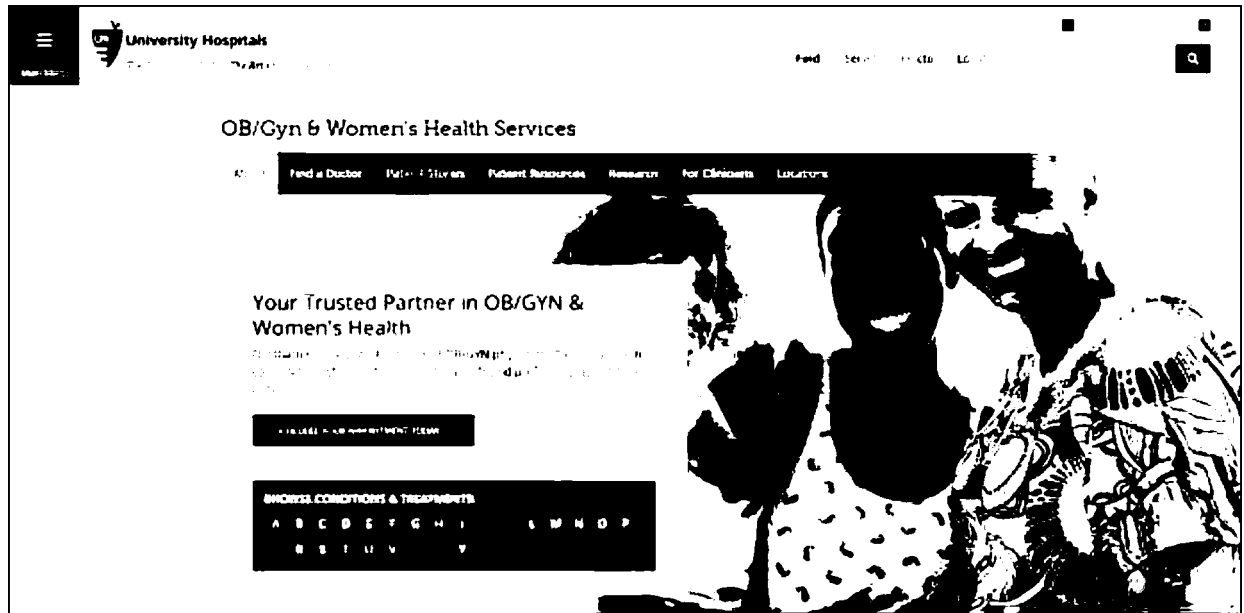
56. UH's use of Google Tag Manager source code is intentionally designed to be invisible. For example, on its "Women's Health Services" page, the Google Tag Manager source code deployed by UH specifies that the "iframe" on the page has a height of 0, a width of 0, display of none, and visibility of "hidden."

79	<!-- Google Tag Manager (noscript) -->
80	<noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-MT6S4R8"
81	height="0" title="google" width="0" style="display:none;visibility:hidden"></iframe></noscript>
82	<!-- End Google Tag Manager (noscript) -->

57. UH then funnels invisible 1x1 web bugs or pixels through this purposefully invisible iframe to transmit patient data and communications to third parties for marketing purposes.



58. Because UH uses an invisible iframe to hide its web bugs, none of the tracking is visible or disclosed to patients on the UH website. Instead, the data transmissions are accomplished through invisible pixels inside of an invisible iframe:



59. UH places the Google Tag Manager source code in the header of its webpages because coding a webpage in this manner reduces the chances that their patients would be able to successfully prevent the disclosures even if they attempt to do so.

60. In addition to placing the Google Tag Manager source code in the header, it appears that UH places source code from Facebook, Invoca, Microsoft, and LPSN Media within its Google Tag Manager program.

### **The Facebook Pixel**

61. UH secretly deploys the Facebook Pixel program on its website.

62. The Facebook Pixel, a product for Facebook Business, is a “piece of code” that lets developers “measure, optimize, and build audiences for ... ad campaigns.”<sup>5</sup>

<sup>5</sup> <https://www.facebook.com/business/learn/facebook-ads-pixel>



63. The Facebook Pixel works through an invisible 1x1 gif as explained above.
64. UH deploys the Facebook Pixel through its invisible Google Tag Manager iframe.
65. Key features of the Facebook Pixel include its ability to help developers:
- a. “Measure cross-device conversions” and “understand how your cross-device ads help influence conversion”;
  - b. “Optimize delivery to people likely to take action” and “ensure your ads are shown to the people most likely to take action”; and
  - c. “Create custom audiences from website visitors” and create “dynamic ads [to] help you automatically show website visitors the products they viewed on your website – or related ones.”
66. Facebook warns developers that the Facebook Pixel causes transmission of personally identifiable information because it “relies on Facebook cookies, which enable [Facebook] to match your website visitors to their respective Facebook User accounts.”

## Implementation

The Facebook pixel is a snippet of JavaScript code that loads a small library of functions you can use to track Facebook ad-driven visitor activity on your website. It relies on Facebook cookies, which enable us to match your website visitors to their respective Facebook User accounts. Once matched, we can tally their actions in the Facebook Ads Manager and Analytics dashboard, so you use the data to analyze your website's conversion flows and optimize your ad campaigns.

67. Facebook further explains “How the Facebook Pixel Works”:

### How the Facebook pixel works

When someone visits your website and takes an action (for example, buying something), the Facebook pixel is triggered and reports this action. This way, you'll know when a customer took an action after seeing your Facebook ad. You'll also be able to reach this customer again by using a custom audience. When more and more conversions happen on your website, Facebook gets better at delivering your ads to people who are more likely to take certain actions. This is called conversion optimization.



68. Facebook recommends that the pixel code be placed early in the source code for any given web page or website to ensure that the user will be tracked:

### **Installing The Pixel**

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

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

69. Through the source code deployed by UH, the cookies that it uses to help Facebook identify patients include, but are not necessarily limited to, cookies named: c\_user, datr, fr, and fbp.

70. The c\_user cookie is a means of identification for Facebook users. The c\_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user account has one – and only one – unique c\_user cookie. Facebook uses the c\_user cookie to record user activities and communications.

71. A skilled computer user can obtain the c\_user cookie value for any Facebook user through the following steps: (1) going to the user's Facebook page, (2) right-clicking on their mouse, (3) selecting 'View page source,' (4) executing a control-F function for "fb://profile," and (5) copying the number value that appears after "fb://profile" in the page source code of the target Facebook user's page.

72. It is even easier to find the Facebook account associated with a c\_user cookie: one simply needs to log-in to Facebook, and then type www.facebook.com/#, with # representing the c\_user cookie identifier. For example, the c\_user cookie value for Mark Zuckerberg is 4. Logging



in to Facebook and typing [www.facebook.com/4](http://www.facebook.com/4) in the web browser retrieves Mark Zuckerberg's Facebook page: [www.facebook.com/zuck](http://www.facebook.com/zuck).

73. The datr cookie identifies a patient's specific web browser from which the patient is sending the communication. It is an identifier that is unique to the patient's specific web browser and is therefore a means of identification for Facebook users. Facebook keeps a record of every datr cookie identifier associated with each of its users, and a Facebook user can obtain a redacted list of all datr cookies associated with his or her Facebook account from Facebook.

74. The fr cookie is a Facebook identifier that is an encrypted combination of the c\_user and datr cookies.<sup>6</sup>

75. The fbp cookie is a Facebook identifier that is set by Facebook source code and associated with UH's use of the Facebook Pixel program. The fbp cookie is a Facebook cookie that masquerades as a first-party cookie to evade third-party cookie blockers and share data more directly between UH and Facebook.

76. Facebook promises users that it requires partners who use Facebook Business Tools to "have lawful rights to collect, use, and share your data before providing any data" to Facebook.

77. Although it has the technological capabilities of ensuring that its partners actually have the lawful rights to collect, use, and share user data before providing it, Facebook does not actually *require* its partners to do so.

78. Instead, Facebook places a provision in its purported form contract with web developers that instructs developers such as UH to "obtain adequate consent" before using the Facebook Pixel.

---

<sup>6</sup> See Facebook Tracking Through Social Plug-ins: Technical Report prepared for the Belgian Privacy Commission, Mar. 27, 2015, available at [https://securehomes.esat.kuleuven.be/~gacar/fb\\_tracking/fb\\_pluginsv1.0.pdf](https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf).



79. According to Facebook, “adequate consent” means UH must make “appropriate disclosures ... [t]hat third parties, including Facebook, may use cookies, web beacons, and other ... technologies to ... receive information from” UH. Facebook Platform Policy at ¶ 2.8. In another provision, Facebook instructs developers to provide “robust and sufficient prominent notice” everywhere that the Facebook Pixel is used. Facebook Business Tools Terms at ¶ 3.

80. UH fails to follow Facebook’s standards for obtaining consent.

### **Other Personally Identifiable Tracking Data**

81. In addition to first- and third-party cookie values, UH uses and permits the following other personally identifiable data to be sent to and accessed by Facebook:

- a. Patient IP addresses;
- b. Patient User-Agent identifiers; and
- c. Patient browser fingerprints.

82. These data elements are all personally identifiable as a matter of law and fact:

- a. HIPAA defines personally identifiable information to include “any unique identifying number, characteristic or code” and specifically lists the examples of medical record numbers, account numbers, device identifiers, serial numbers, URLs and IP addresses. *See* 45 C.F.R. § 164.514(2).
- b. HIPAA further declares information as personally identifiable where the covered entity has “actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.” 45 C.F.R. § 164.514(2)(ii).
- c. Ohio has adopted the HIPAA definitions in Ohio Rev. Code § 3798.04.



- d. To Plaintiff's knowledge, every federal agency charged with rulemaking to determine the definition of personally identifiable information has found that the types of data used and disclosed by UH are personally identifiable.

***Patient IP Addresses are Personally Identifiable***

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

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

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

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

87. Google tracks IP addresses associated with specific Internet users.

88. The other third-party marketing companies that UH procured to obtain the contents of patient communications associate particular IP addresses with specific Internet users.

89. Individual homes and their occupants can be, and are, tracked and targeted with advertising using IP addresses.

90. Under HIPAA, an IP address is considered personally identifiable information. *See* 45 C.F.R. § 164.514(b)(2)(i)(O).

91. UH uses and causes the disclosure of patient IP addresses to third parties with each re-directed communication described herein, including patient communications within the MyUHCare Patient Portal, on the Patient Portal log-in page, and communications concerning individual providers, conditions, and treatments.

92. In addition to disclosing IP addresses, UH uses and causes the disclosure of patient User Agent information. The User Agent information identifies the application, operating system,



and version of the patient's device. In a household with more than one computer, the IP address would identify the household and the User Agent would distinguish the different devices within the household.

***Internet Cookies are Personally Identifiable***

93. In the early years of the Internet, advertising on websites followed the same model as traditional newspapers. Just as a sporting goods store would choose to advertise in the sports section of a traditional newspaper, advertisers on the early Internet paid for ads to be placed on specific web pages based on the type of content displayed on the web page.

94. Computer programmers eventually developed 'cookies' – small text files that web servers can place on a person's web browser and computing device when that person's web browser interacts with the website server. Some cookies are designed to acquire and record an individual Internet user's communications and activities on websites across the Internet.

95. Cookies are designed to, and, in fact, do operate as means of identification for Internet users.

96. Cookies are protected personal identifiers under HIPAA. *See* 45 C.F.R. § 164.514(b)(2)(i)(H), (J), (M), (N), and (R).

97. In general, cookies are categorized by (1) duration and (2) party.

98. There are two types of cookies classified by duration:

- a. "Session cookies" are placed on a user's computing device only while the user is navigating the website that placed and accesses the cookie. The user's web browser typically deletes session cookies when the user closes the browser.



- b. “Persistent cookies” are designed to survive beyond a single Internet-browsing session. The party creating the persistent cookie determines its lifespan. As a result, a persistent cookie can acquire and record a user’s Internet communications for years and over dozens or hundreds of websites. Persistent cookies are sometimes called “tracking cookies.”

99. Cookies are also classified by the party that uses the collected data.

- a. “First-party cookies” are set on a user’s device by the website with which the user is exchanging communications. For example, UH sets a collection of its own cookies on patients’ browsers when they visit any web page on the UH website. First-party cookies can be helpful to the user, server, and/or website to assist with security, log in, and functionality.
- b. “Third-party cookies” are set on a user’s device by website servers other than the website or server with which the user is exchanging communications. For example, the same patient who visits UH will also have cookies on their device from third parties, such as Facebook. Unlike first-party cookies, third-party cookies are not typically helpful to the user. Instead, third-party cookies are typically used for data collection, behavioral profiling, and targeted advertising.

100. Data companies like Facebook have developed methods for monetizing and profiting from cookies. These companies use third-party tracking cookies to help them acquire and record user data and communications in order to sell advertising that is customized to that person’s communications and habits. To build individual profiles of Internet users, third-party data companies assign each user a unique, or a set of unique identifiers to each user.



101. UH uses and causes the disclosure of patient cookie identifiers to third parties with each re-directed communication described herein, including patient communications on the patient-portal log-in page and communications concerning individual providers, conditions, and treatments.

***Browser-Fingerprints are Personally Identifiable***

102. A browser fingerprint is information collected about a computing device that can be used to identify the device.

103. A browser fingerprint can be used to identify a device when the device's IP address is hidden and cookies are blocked.

104. The Electronic Frontier Foundation has explained:

When a site you visit uses browser fingerprinting, it can learn enough information about your browser to uniquely distinguish you from all the other visitors to that site. Browser fingerprinting can be used to track users just as cookies do, but using much more subtle and hard-to-control techniques. In a paper EFF released in 2010, we found that a majority of users' browsers were uniquely identifiable given existing fingerprinting techniques. Those techniques have only gotten more complex and obscure in the intervening years. By using browser fingerprinting to piece together information about your browser and your actions online, trackers can covertly identify users over time, track them across websites, and building an advertising profile of them.<sup>7</sup>

105. Google recently explained, "With fingerprinting, developers have found ways to use tiny bits of information that vary between users, such as what device they have or what fonts they have installed to generate a unique identifier which can then be used to match a user across websites. Unlike cookies, users cannot clear their fingerprint, and therefore cannot control how their information is collected."<sup>8</sup>

---

<sup>7</sup> Katarzyna Szymielewicz and Bill Dudington, Electronic Frontier Foundation, The GDPR and Browser Fingerprinting: How It Changes the Game for the Sneakiest Web Trackers, <https://www.eff.org/deeplinks/2018/06/gdpr-and-browser-fingerprinting-how-it-changes-game-sneakiest-web-trackers>.

<sup>8</sup> <https://www.blog.google/products/chrome/building-a-more-private-web/>



106. In 2017, researchers showed that browser fingerprinting techniques can successfully identify 99.24 percent of users.<sup>9</sup>

107. Browser fingerprints are protected personal identifiers under HIPAA. *See* 45 C.F.R. § 164.514(b)(2)(i)(M), (R).

108. UH uses and causes the disclosure of data sufficient for third parties to create a browser-fingerprint identifier with each re-directed communication described herein, including patient communications within the Patient Portal and on the patient-portal log-in page, and communications concerning individual providers, conditions, and treatments.

#### **THE THIRD PARTIES TO WHOM UH MAKES DISCLOSURES**

##### ***Google***

109. By many measures, Google is the world's largest data company. Among other services, Google operates the world's most popular search engine (Google), email provider (Gmail), video website (YouTube), mapping service (Google Maps), Internet analytics service for web developers (Google Analytics), and web browser (Chrome). It also operates various ad services that are among the world's most popular in their respective categories, including the advertising services of Google DoubleClick and Google AdWords.

110. Google Analytics has massive reach. As described by *The Wall Street Journal*, it is “far and away the web’s most dominant analytics platform” and “tracks you whether or not you are logged in.”<sup>10</sup>

---

<sup>9</sup> Yinzhi Cao, Song Li, Erik Wijmans, (Cross-)Browser Fingerprinting via OS and Hardware Level Features, Proceedings of the Network and Distributed Security Symposium, March 2017, available at [http://yinzhihao.org/TrackingFree/crossbrowsertracking\\_NDSS17.pdf](http://yinzhihao.org/TrackingFree/crossbrowsertracking_NDSS17.pdf).

<sup>10</sup> *Who Has More of Your Personal Data than Facebook? Try Google*, *The Wall Street Journal*, <https://www.wsj.com/articles/who-has-more-of-your-personal-data-than-facebook-try-google-1524398401>.



111. Google tracks Internet users with IP addresses, cookies, geolocation, and other unique device identifiers.


112. Google warns web developers that Google marketing tools are not appropriate for every type of website or webpage, including health-related webpages and websites.

113. To deploy the Google Remarketing tools, UH obtains Google source code from Google and places it on the UH website directly or through a tag manager.

114. By following the instructions in the Google source code, a developer is warned that “Health in personalized advertising” is a “Prohibited category” for Google’s personalized advertising tools. Specifically, Google’s advertising policies page states:<sup>11</sup>

We take user privacy very seriously, and we also expect advertisers to respect user privacy. These policies define how advertisers are allowed to collect user data and use it for personalized advertising. They apply to advertisers using targeting features, including remarketing, affinity audiences, custom affinity audiences, in-market audiences, similar audiences, demographic and location targeting, and keyword contextual targeting. ...

You aren’t allowed to do the following:

 Collect information related to sensitive interest categories (see Personalized advertising policy principles below for more about sensitive interest categories)
--

Google further states that “[a]dvertisers can’t use sensitive interest categories to target ads or to promote advertisers’ products or services.” “Health” is a “[p]rohibited categor[y]” that Google states “can’t be used by advertisers to targets ads to users or promote advertisers’ products or services.”

---

<sup>11</sup> <https://support.google.com/adspolicy/answer/143465?hl=en>



## Health in personalized advertising

✖ Personal health conditions, health issues related to intimate body parts or functions, and invasive medical procedures. This also includes treatments for health conditions and intimate bodily health issues.

- Examples: treatments for chronic health conditions like diabetes or arthritis, treatments for sexually transmitted diseases, counseling services for mental health issues like depression or anxiety, medical devices for sleep apnea like CPAP machines, over-the-counter medications for yeast infections, information about how to support your autistic child

Health content includes:

- physical or mental health conditions, including diseases, chronic conditions, and sexual health
- health condition-related services or procedures
- products for treating or managing health conditions, including over-the-counter medications for health conditions and medical devices
- long or short-term health issues associated with intimate body parts or functions, including genital, bowel, or urinary functions
- invasive medical procedures, including cosmetic surgery
- disabilities, even when content is oriented toward the user's primary caretaker

115. Google, however, violates its own restrictions on remarketing.

116. Google provides instructions for web developers to anonymize IP addresses when they use Google Analytics.<sup>12</sup> Google explains that the IP anonymization feature “is designed to help site owners comply with their own privacy policies, or, in some countries, recommendations from local data protection authorities, which may prevent the storage of full IP address information.” The Google IP anonymization instructions tell web developers to add a parameter called ‘aip’ in their Google Analytics source code. When ‘aip’ (“anonymize IP”) is turned on, it will be reported to Google Analytics in a GET request with the following: ‘&aip=1.’

117. UH does not use Google’s IP anonymization tool with Google Analytics. As a result, UH’s use of Google Analytics is not anonymous, even when no cookies are involved in the re-direction of a patient’s communication.

---

<sup>12</sup> Available at <https://support.google.com/analytics/answer/2763052?hl=en>



118. UH deploys Google tracking tools on nearly every page on its website, thereby causing disclosure of communications exchanged with patients to be re-directed to Google. The re-directed patient communications include communications that patients make:

- a. On the patient portal log-in page at MyUHCare; and
- b. At UH.com that pertain to the patient's communications regarding specific providers, conditions, treatments, and appointment requests.

119. UH has specifically implemented the Google Analytics remarketing function to cause disclosures of communications that patients make within the Patient Portal.

### ***Facebook***

120. Facebook operates the world's largest social media company.

121. Facebook maintains profiles on users that include user's real names, locations, email addresses, friends, likes, and communications that Facebook associates with personal identifiers, including IP addresses and cookie identifiers.

122. Facebook also tracks non-users across the web through its widespread Internet marketing products and source code.

123. Facebook's revenue is derived almost entirely from selling targeted advertising to its users on Facebook.com and to all Internet users on non-Facebook sites that integrate Facebook marketing source code on their websites.

124. Facebook Business is the division that provides advertising services to developers.

125. The Facebook Pixel, described above, is a tool within Facebook Business.

### ***Microsoft***

126. Though best known for its software, Microsoft also sells digital advertising through a domain associated with its search engine, Bing.com.



127. Microsoft tracks users through IP addresses and persistent cookies.

128. UH deploys Microsoft source code on the UH home page and pages relating to patient communications about specific medical providers, conditions, and appointment requests.

### ***LivePerson***

129. LivePerson provides methods through which companies can communicate with their consumers over a variety of communications channels.

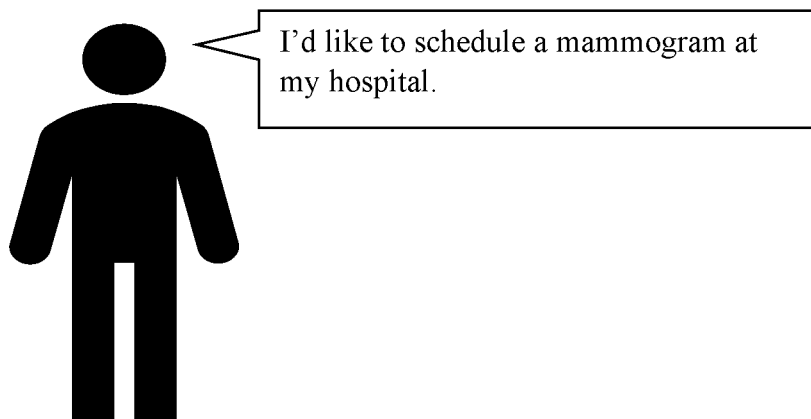
130. LivePerson tracks consumers, including patients at the UH website, with IP addresses and cookie identifiers.

131. UH deploys LivePerson source code on all parts of the UH website, including pages relating to patient communications about specific medical providers, conditions, and appointment requests.

### **HOW UH DISCLOSES PERSONALLY IDENTIFIABLE, NON-PUBLIC MEDICAL INFORMATION TO THIRD PARTIES DURING A ROUTINE APPOINTMENT SCHEDULING**

132. The following illustrates a series of typical communications between a patient and UH, and how UH secretly discloses unauthorized personally identifiable, non-public patient information, and the content of their communications to Facebook and others.

133. The interaction between the patient and UH begins when the patient decides to schedule a mammogram at UH:





134. The patient can begin the process through one of two typical methods. The patient can either perform a search using the embedded search functionality on UH's website, or it can navigate through UH's website through a series of subpages.

135. If a patient chose to navigate through UH's website to learn about their breast cancer diagnosis, consider treatment options, and, ultimately, schedule an appointment with their doctor, UH discloses *all of this information* to Facebook and other third parties, in real-time, connected to personally identifiable information about the patient.

***Step 1: The Patient Visits [www.uhhospitals.org](http://www.uhhospitals.org)***

136. First, the patient starts at UH's main webpage, located at [www.uhhospitals.org](http://www.uhhospitals.org):

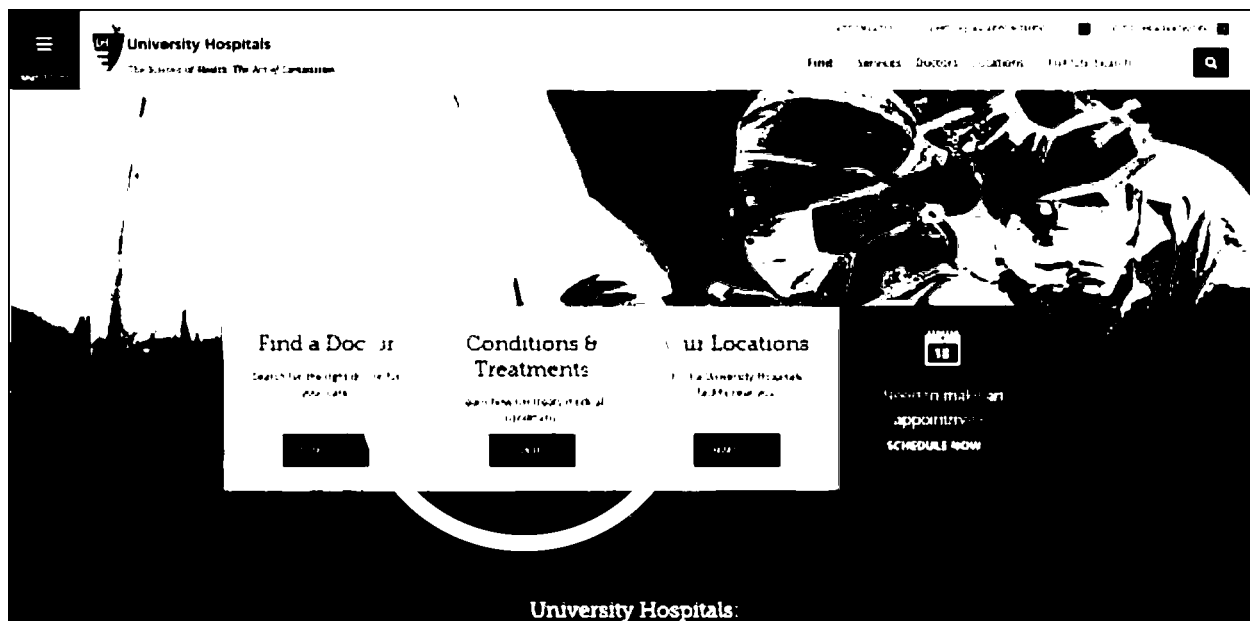


137. The fact that the patient is at the UH web property is contemporaneously transmitted to Facebook and other third parties.



***Step 2: The Patient Clicks on “Search” for “Conditions & Treatments”***

138. From there, the patient clicks on “Conditions & Treatments” to begin their review of the breast cancer treatment options UH has available for its patients:



139. As soon as the patient clicks on “Search” under “Conditions & Treatments,” UH begins the process disclosing the patient’s personally identifiable, non-public medical information to third parties through a ‘GET’ request.

140. UH discloses to Facebook that the patient clicked to send a Search query under Conditions & Treatments through an ‘ev’, called a SubscribedButtonClick.

141. UH’s re-direction of the SEARCH communication to Facebook is done without the patient’s knowledge, consent, authorization, or privilege.



142. The following is a screenshot of some of the data UH transmits to Facebook:

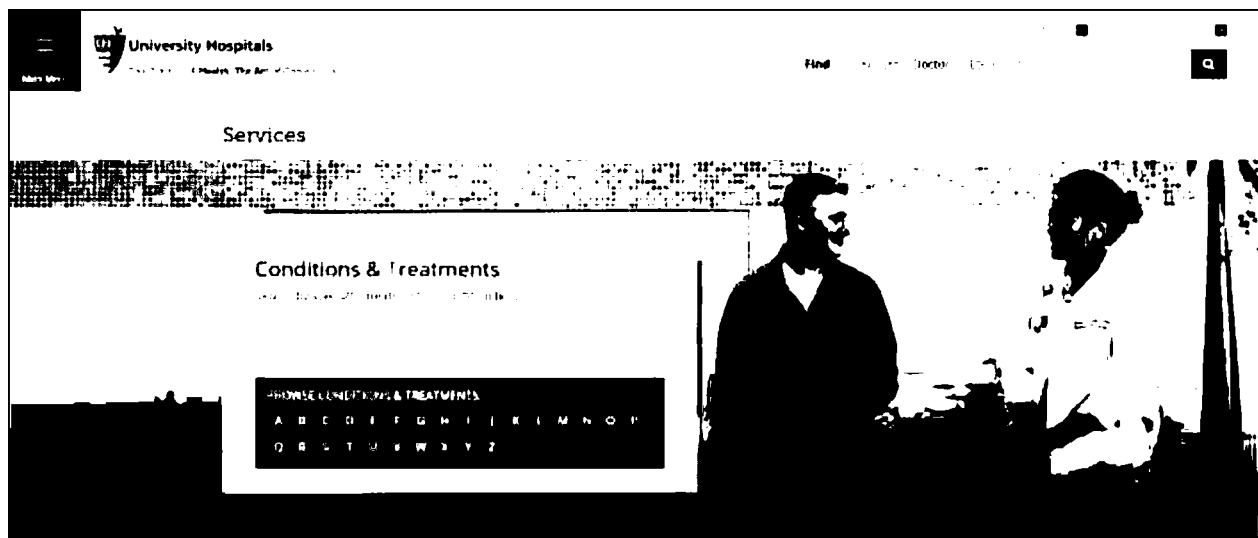
Name	Value
id	[REDACTED]
ev	SubscribedButtonClick
dl	https://www.uhhospitals.org/
rl	
if	false
ts	1582040065442
cd[buttonFeatures]	{"classList":["UH-Button-Secondary","destination":"","id":"","imageUrl":"","innerText":"SEARCH","numChildButtons":
cd[buttonText]	SEARCH
cd[formFeatures]	{}
cd[pageFeatures]	{"title":"Nationally Ranked Healthcare - Largest Network of Hospitals, Doctors & Surgeons in Cleveland & Northeast Ohio   University Hospitals"}
cd[parameters]	{}
sw	1280
sh	720
v	2.9.15
r	stable
ec	2
o	30
fbp	fb.1 [REDACTED]
it	[REDACTED]

143. In addition to this data, UH transmits to Facebook the patient's IP address, User Agent data, information sufficient to form a browser fingerprint, and unique persistent Facebook cookies values.

144. From this disclosure, UH has informed Facebook that a specific individual has engaged in a "SubscribedButtonClick" which represents them having clicked on the "SEARCH" button located on the UH home page at <https://www.uhhospitals.org/>.

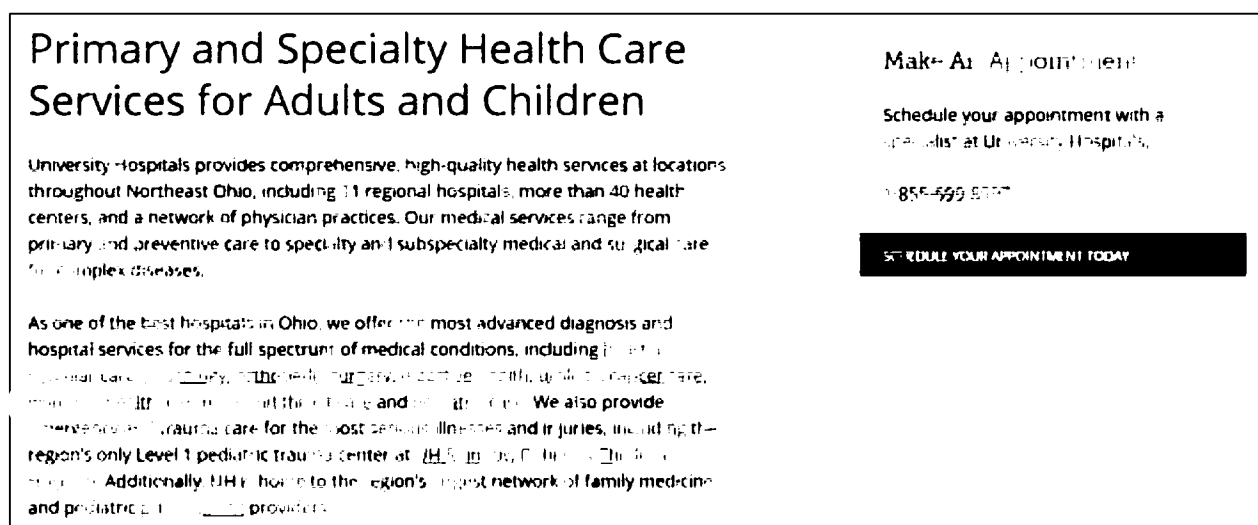


145. Meanwhile, from the patient's perspective, the only thing they see is the following page load on their screen:



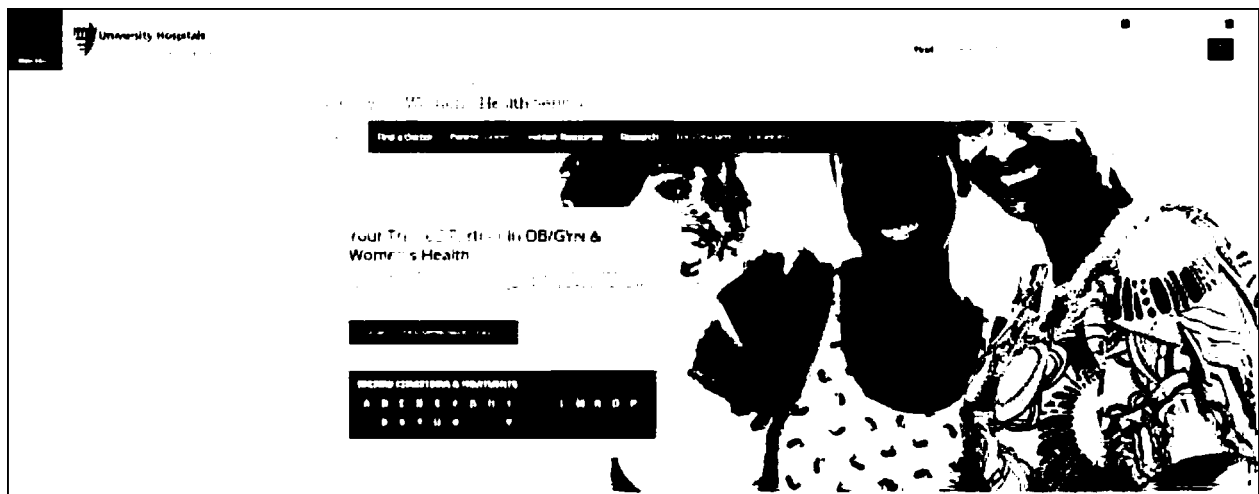
***Step 3: The Patient Visits the “Women’s Health” Division on UH’s Medical Services***

146. On the “Conditions & Treatments” landing page for the “Search” button, the patient can navigate to several individual pages providing additional information about specific services provided by the hospital. Towards the bottom of the webpage, the patient can link to the “women’s health” division of the website in order to look further into UH’s breast cancer services:

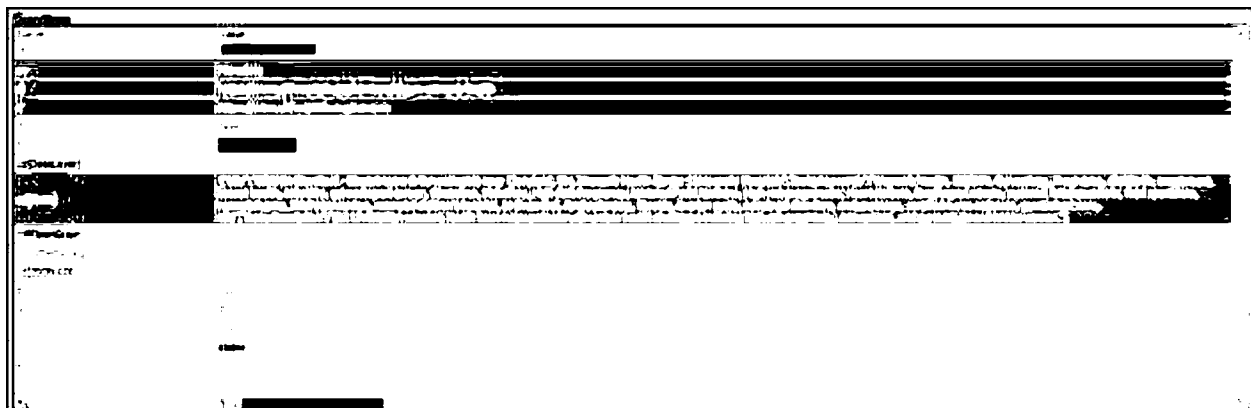




147. The “women’s health” link then sends the patient to the “OB/GYN & Women’s Health Services” page:



148. Once again, UH discloses the microdata of the patient’s communications with UH to Facebook, revealing that a specific individual visited the “Women’s Health Center” which “helps patients with unique health challenges including . . . breast cancer”:



***Step 4: The Patient Visits the “Breast Center of Excellence” to Find Out About the Treatment Options at Her Hospital***

149. Scanning further down the “OB/GYN & Women’s Health” page leads the patient to the “Women’s Breast Health” area of UH, with a link to the “Breast Center of Excellence.” UH’s Breast Center of Excellence touts itself as “provid[ing] innovative and personal care aimed

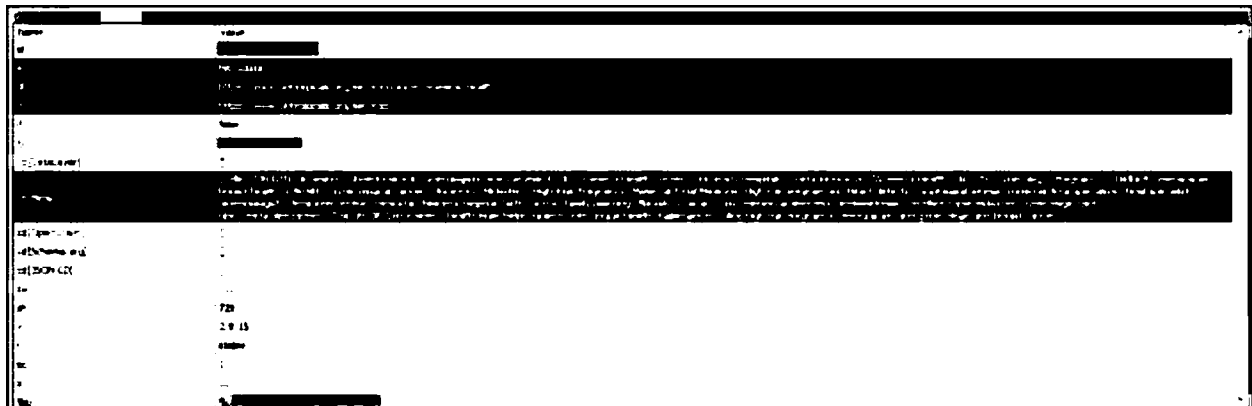


at preventing, diagnosing and treating breast conditions, from benign (noncancerous) to malignant (cancerous) breast disease including several types of breast cancer[.]”:

### Women’s Breast Health

University Hospitals provides innovative and personal care aimed at preventing, diagnosing and treating breast conditions, from benign (noncancerous) to malignant (cancerous) breast disease including several types of breast cancer. We offer board-certified breast care specialists recognized as experts in the field, and an accredited Breast Center of Excellence designated by the American College of Radiology. With locations across northeast Ohio, our team specializes in tomosynthesis (a digital 3D mammogram), breast ultrasound, ultrasound-guided breast biopsy, stereotactic biopsy and breast magnetic resonance imaging (MRI).

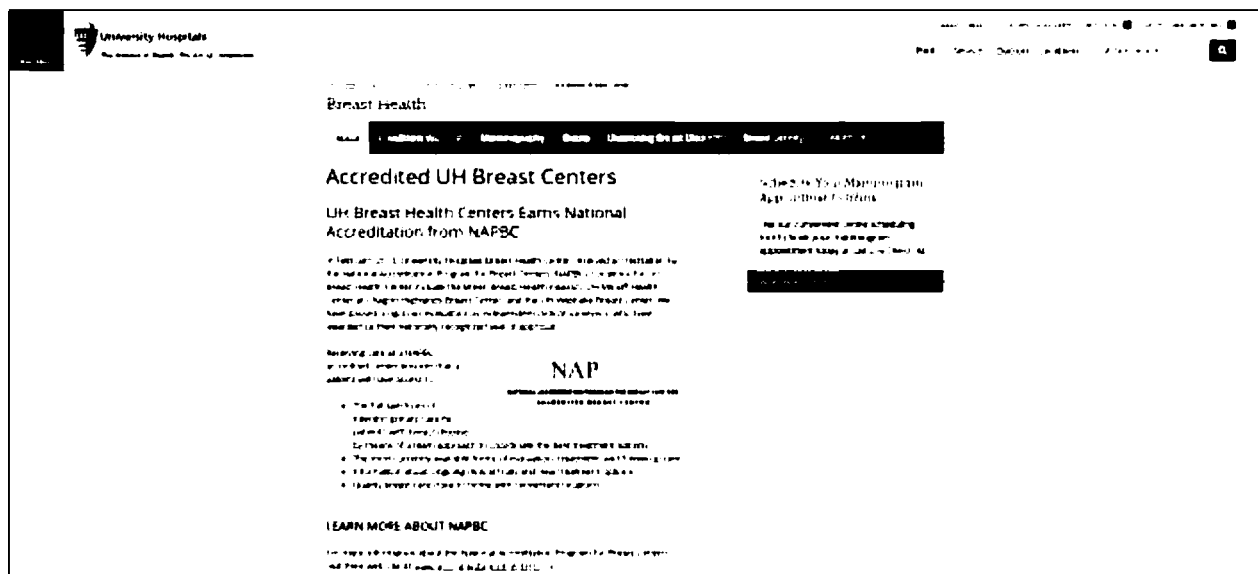
150. Upon clicking on the “Breast Center of Excellence” link to officially enter the Center’s website and begin scheduling an appointment, the patient is sent to <https://www.uhhospitals.org/services/obgyn-womens-health/breast-health/accredited-breast-center>, which UH immediately discloses to Facebook:



151. Meanwhile, the patient remains unaware that UH is sharing its personally identifiable, non-public medical information regarding her diagnosis and treatment with Facebook

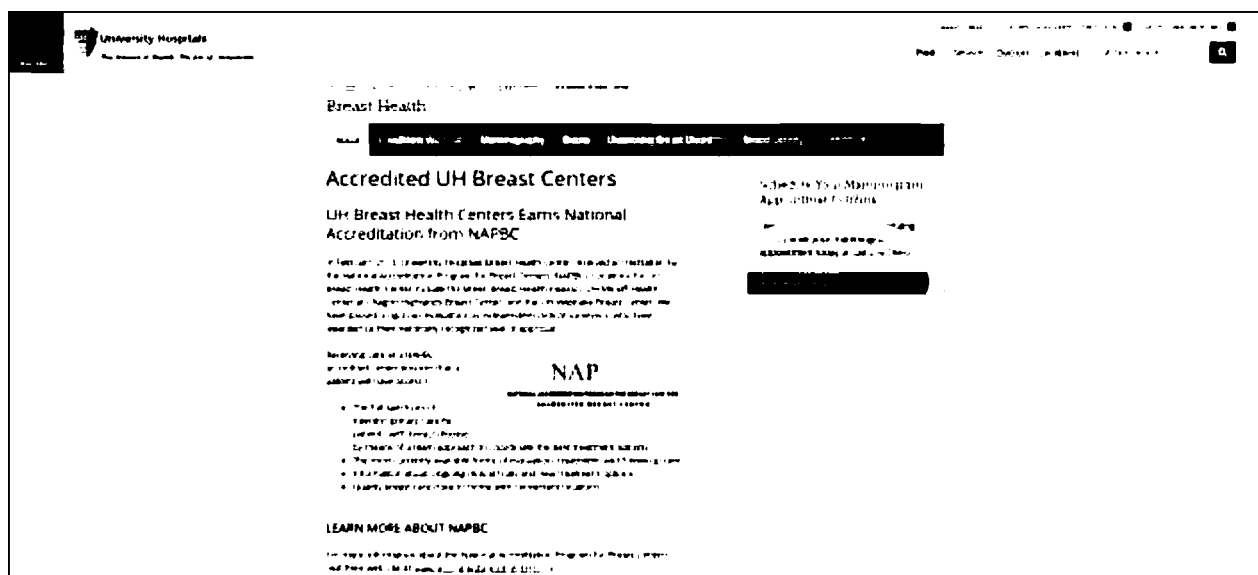


as she navigates UH's website. Rather, the patient only sees the UH's substantive responsive communication, which does not reveal its secret disclosures:



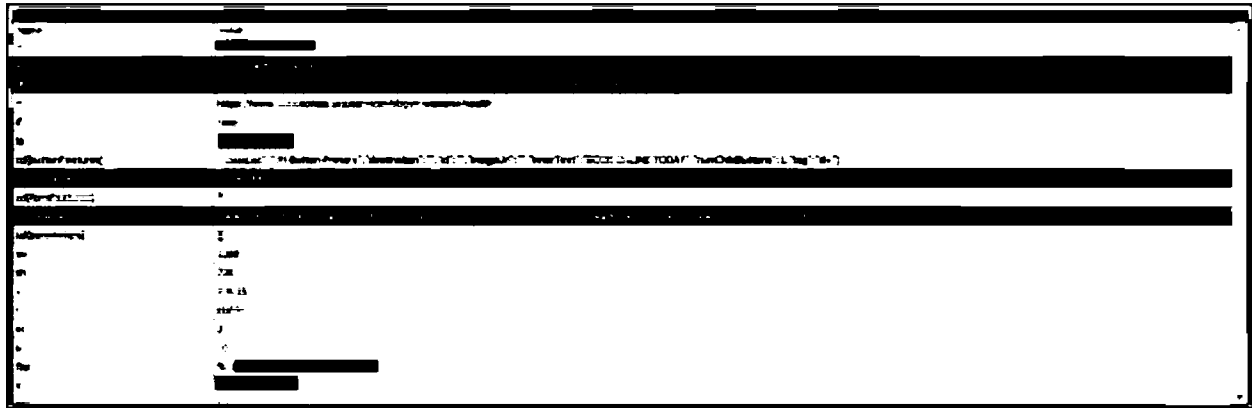
***Step 5: UH Informs Facebook That the Patient is Scheduling an Appointment on a Specific Day, at a Specific Location, With a Specific Department, for a Specific Treatment***

152. UH encourages patients to use its “convenient online scheduling tool to book your mammogram appointment” via a link placed directly on the Breast Health’s webpage:





153. Unbeknownst to the patient, UH secretly shares the patient's scheduling communications with Facebook in real time and in plain English. First, UH tells Facebook that the patient has opted to "book online today" through a SubscribedButtonClick:



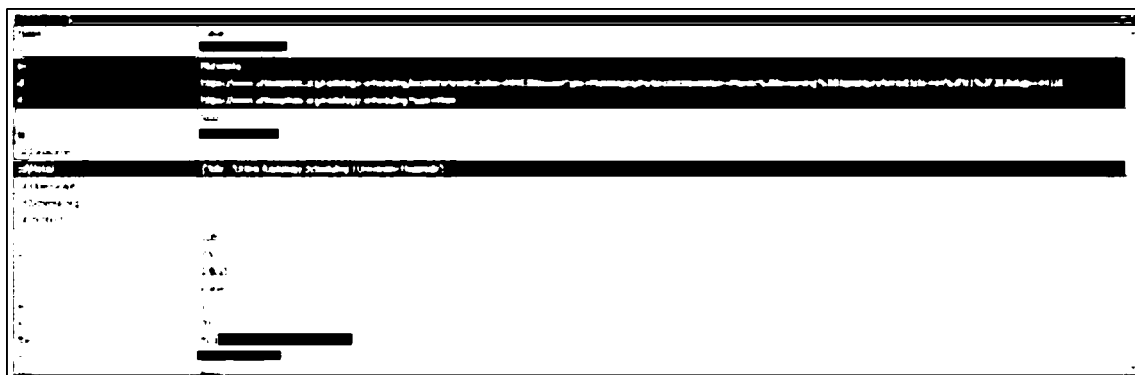
154. Next, UH presents the patient to a fillable web form – the contents of which are shared with Facebook. UH even informs Facebook whether the patient is scheduling the appointment on their behalf or for someone else.

155. For example, if a patient tells UH that they are over the age of 35 and attempts to schedule their mammogram appointment with radiology on April 1, 2020 in the 44122 area, the patient would complete the form as follows:

A screenshot of the University Hospitals 'Schedule Your Radiology Appointment' web form. The form is titled 'Schedule Your Radiology Appointment' and includes fields for 'First Name', 'Last Name', 'Email', 'Phone', 'Address', 'City', 'State', 'Zip', 'Age', 'Gender', 'Race', 'Ethnicity', 'Language', 'Religion', 'Sexual Orientation', 'Marital Status', 'Insurance', 'Referral', 'Referral Source', 'Referral Date', 'Referral Doctor', 'Referral Facility', 'Referral Address', 'Referral City', 'Referral State', 'Referral Zip', 'Referral Phone', 'Referral Email', 'Referral Website', 'Referral Notes', 'Referral Comments'. The form is partially filled out with a patient's information.



156. Yet, UH secretly discloses all of this non-public medical information directly from the forms themselves to Facebook as microdata along with HIPAA personally identifiable information in the form of their c\_user, datr, fr, and fbp cookies, their IP address and User Agent, and browser fingerprint information:



157. Upon close inspection, UH's disclosure reveals the following non-public medical information pulled directly from the patient's form:

- a. The department the patient is scheduling an appointment with (*i.e.* radiology):

<a href="https://www.uhhospitals.org/radiology-scheduling/locations?ex">https://www.uhhospitals.org/radiology-scheduling/locations?ex</a>
<a href="https://www.uhhospitals.org/radiology-scheduling?type=Mam">https://www.uhhospitals.org/radiology-scheduling?type=Mam</a>
false
[REDACTED]
[REDACTED]
{ "title": "Online Radiology Scheduling   University Hospitals" }

- b. The specific treatment the patient is scheduling (*i.e.* mammogram):

examType=Mammography&examDescription=Mamm%20Screening
---

- c. The location of the appointment (*i.e.* 44122):

zip=44122
-----------



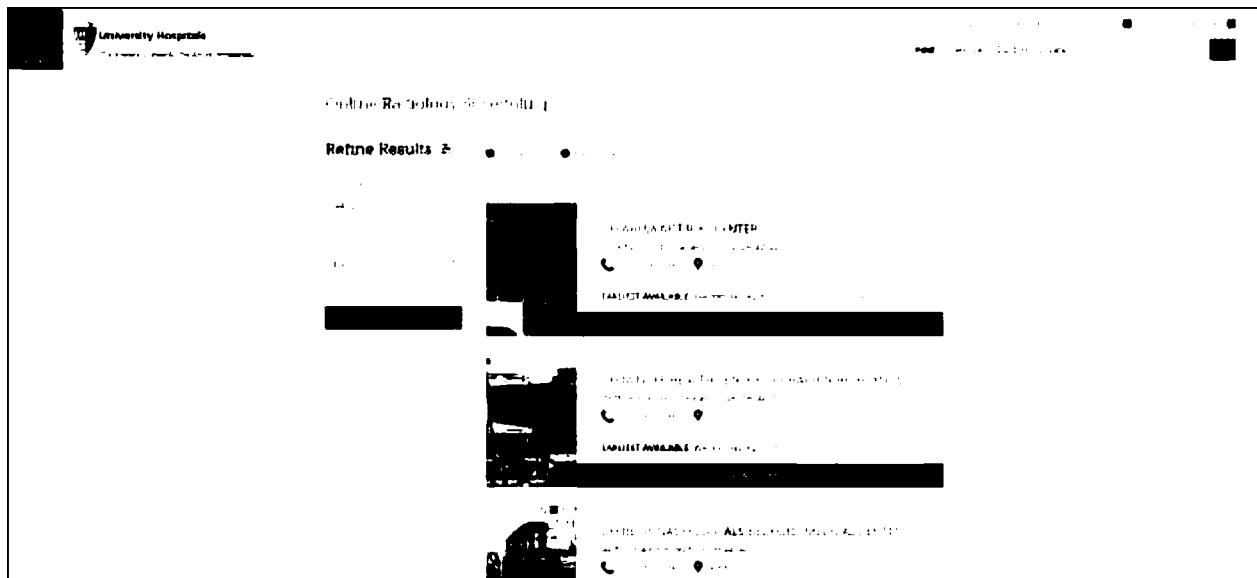
- d. The date of the appointment (*i.e.* 4/1/2020):

preferredDate=04%2F01%2F2020

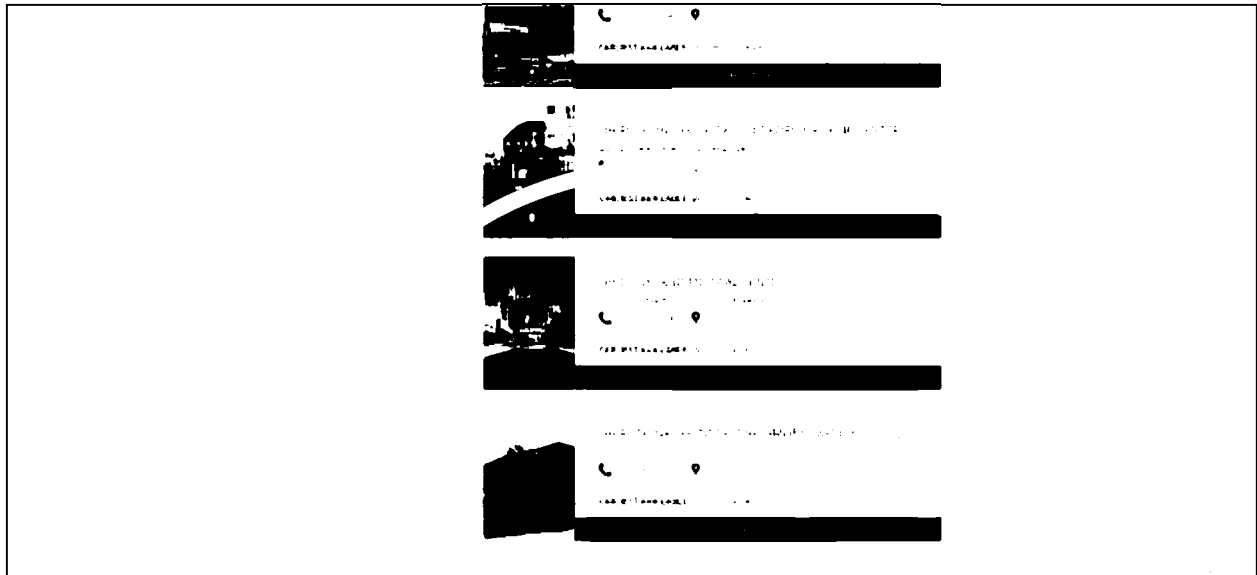
158. When the patient then clicks on the “search” button to select a specific facility and a specific time (having already identified the date and zip code), UH then re-discloses all of this information to Facebook a second time in a nearly identical fashion.

***Step 6: The Patient Selects a Facility and Time for Their Mammogram***

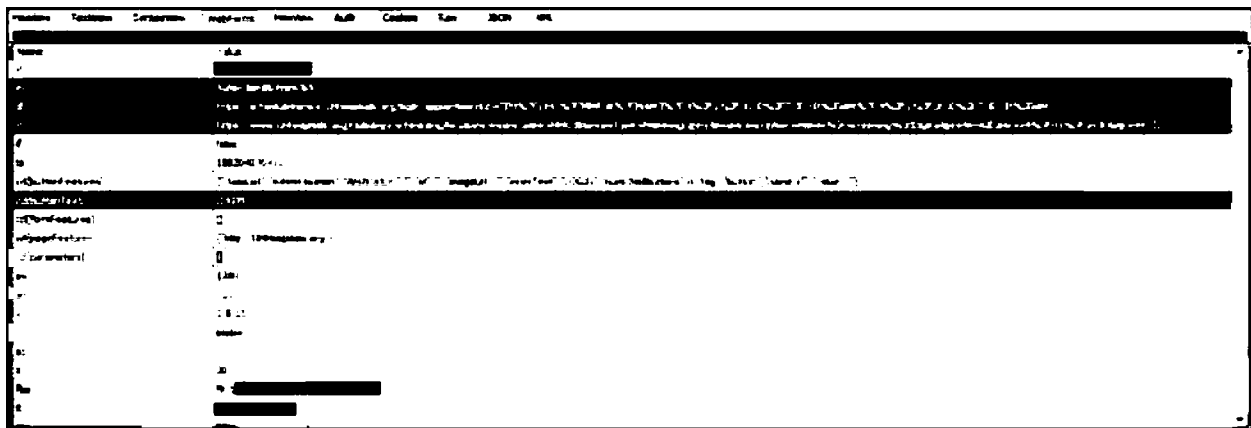
159. Having clicked the “search” button for available appointments, the patient would land on the following options for her mammogram, including, in this case, a 7:30 AM appointment at UH Cleveland Medical Center:





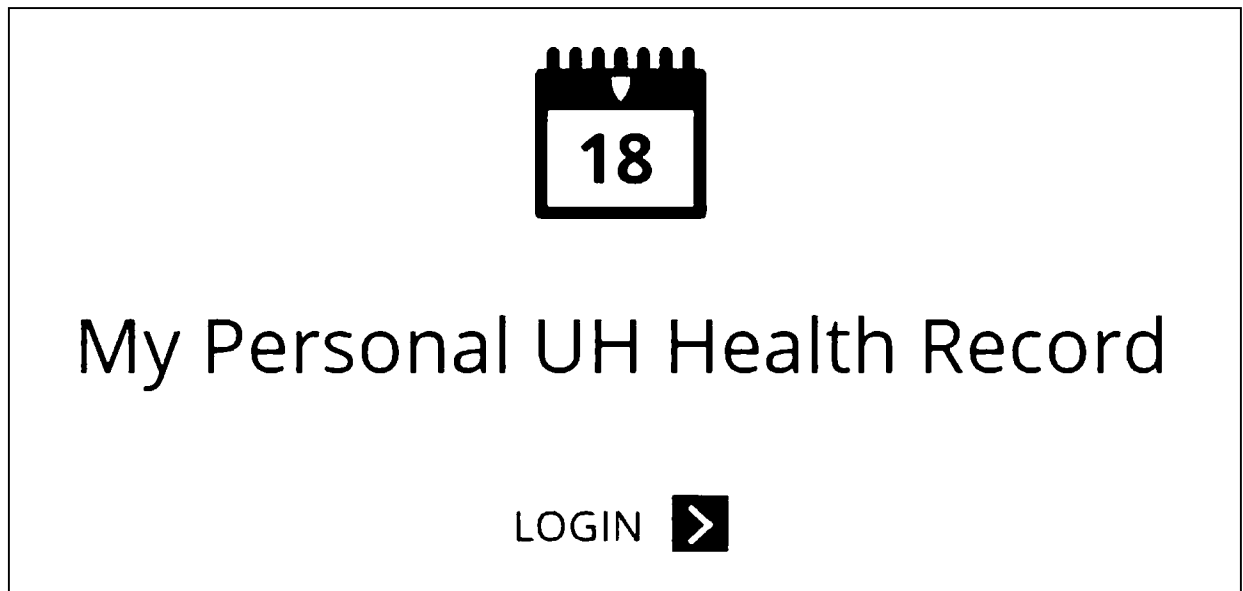


160. Conveniently, UH encourages the patient to book their appointment immediately through its website by clicking on the “7:30 AM” option and logging into their patient portal. Upon a patient doing so, UH discloses everything to Facebook, from the details of their appointment to their patient status:



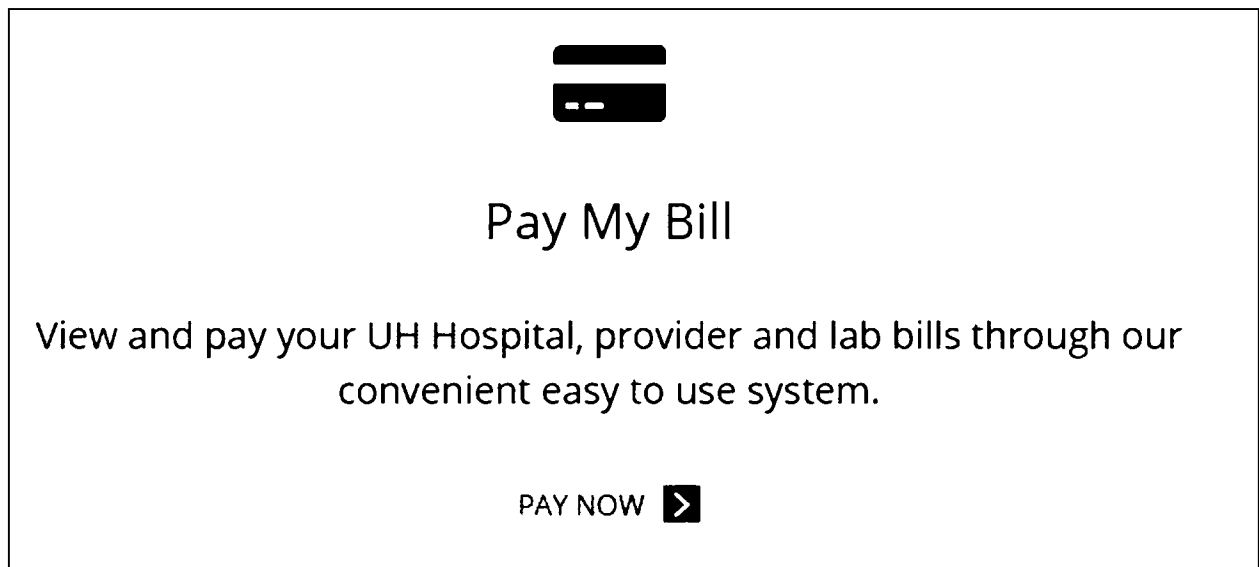


161. UH also disclose every time a patient clicks to log-in to their “Personally UH Health Record” that UH refers to as “MyUHCare”:



162. When a patient clicks to log-in, UH discloses a SubscribedButtonClick event to Facebook that they are now logging-in to the patient portal.

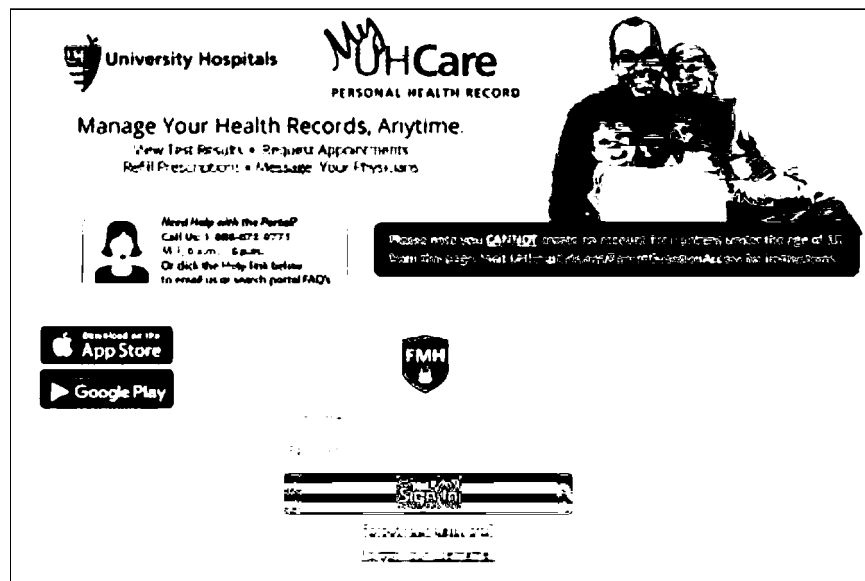
163. Similarly, when a patient clicks to “Pay Now” under a payment process that UH places at its web-property, UH discloses a SubscribedButtonClick event to Facebook that the particular patient has sent a communication to “Pay Now.”





164. UH even discloses the patient's communications on the login page on its patient portal home page:

<https://uhhospitals.followmyhealth.com/Login/Home/Index?authproviders=0&returnArea=PatientAccess#!/default#%2Fdefault:>



165. On this different domain for the patient portal, hosted by followmyhealth.com rather than UH, the source code continues to cause data transmissions from patient computers to Google connected to personally identifiable information about patients, but not to Facebook or the others.

#### **UH MAKES SUBSTANTIALLY SIMILAR DISCLOSURES THROUGHOUT ITS WEB PROPERTY**

166. The same or substantially similar disclosures are made to Facebook, Google, and the other third parties every time a patient exchanges a communication with UH at the UH web property set-up for patients at [www.uhhospitals.org](http://www.uhhospitals.org).



167. Other patient communications regularly disclosed by UH to Facebook, Google, and others include:

- a. Every time a patient views the profile page for their doctor or potential doctor;
- b. Every time a patient clicks a link to “Book an Appointment”;
- c. Every time a patient reviews “Services” offered by UH;
- d. Every time a patient uses the UH “symptom checker” tool at <https://www.uhhospitals.org/health-information/health-and-wellness-library/symptom-checker#!/index/child/body>, which causes data transmissions to third parties of all symptoms identified to UH;
- e. Every time a patient looks up information on their specific conditions or treatments and UH’s Health & Wellness library at <https://www.uhhospitals.org/health-information/health-and-wellness-library>;
- f. Every time a patient clicks a link on [www.uhhospitals.org](http://www.uhhospitals.org) to LOGIN to their online patient portal called MyUHCare; and
- g. Every time a patient clicks to “Pay Now”.

**UH’S DISCLOSURES MUST BE CONSIDERED INDIVIDUALLY AND AS A WHOLE**

168. Each of the individual data elements described above is personally identifiable, non-public medical information on their own. However, UH’s disclosures of such personally identifiable, non-public medical elements do not occur in a vacuum. The disclosures of the different data elements are tied together and, when taken together, these data elements are even more accurate in identifying individual patients, particularly when disclosed to data companies



such as Facebook, Google, and others that expressly state they use such data elements to identify individuals.

**UH'S DISCLOSURES ARE NOT PUBLIC INFORMATION**

169. The [www.uhhospitals.com](http://www.uhhospitals.com) web property is publicly available to patients, potential patients, and other Internet users just as UH hospitals are publicly available.

170. The fact that Plaintiff is a patient of UH is not publicly available.

171. The fact that Plaintiff exchanged communications with UH at its web property is not publicly available.

172. The facts that Plaintiff has registered for, used, and exchanged communications with UH inside the MyUHCare patient portal, and the specific data and times associated with those communications, are not publicly available.

173. The specific communications exchanged between Plaintiff and UH, including communications about specific appointments, providers, conditions and treatments, are not publicly available information – regardless of whether such communications occurred before or after Plaintiff or patients had signed in to MyUHCare.

174. The department that provides care for Plaintiff is not publicly available.

175. The treatment that Plaintiff receives is not publicly available.

176. The dates of Plaintiff's appointments are not publicly available.

177. The times of Plaintiff's appointments are not publicly available.

178. The locations of Plaintiff's appointments are not publicly available.

179. The personal information that UH causes to be disclosed to third parties about patients after they have signed in to the MyUHCare portal is not public information.



## **UH IS ENRICHED FOR MAKING THE UNAUTHORIZED DISCLOSURES**

180. The purpose of UH's disclosures and procurement of third parties to intercept patient communications is marketing.

181. In exchange for disclosing personally identifiable, non-public patient data, and communications, UH is compensated by the third parties with enhanced advertising services, including, but not limited to, re-targeting.

182. This barter transaction between UH and the third parties constitutes a sale.

183. As described below, the third parties then work with UH to target patients with advertisements on different websites and different computing devices.

184. The third parties also take the personal information disclosed by UH and the contents of communications and uses them to create detailed profiles on individual consumers that the third parties can and do use for their own purposes.

185. Once the personally identifiable, non-public medical information relating to patients is disclosed to third parties, UH loses the ability to control its further dissemination and use. As described below, several of the third parties share and use data with fourth parties and use data collected from websites such as the UH website to sell marketing products to others.

186. Retargeting is a form of online targeted advertising that targets users with ads based on their previous Internet communication and interactions.

187. Retargeting is facilitated through the deployment of tracking pixels and cookies. Once data is disclosed and shared with a third-party marketing company, the advertiser is able to show ads to the user elsewhere on the Internet.

188. Retargeting enables UH to show advertisements on other websites to patients or potential patients based on specific communications exchanged at UH's property. Using the



Facebook Pixel, UH can target ads on Facebook itself or the Facebook advertising network to patients for whom Facebook recorded actions at UH. The same or similar targeted actions can be accomplished via disclosures to the other third-party marketing companies.

189. In addition to enabling UH to advertise to patients and potential patients on non-UH websites, Defendant's disclosures of patient data and communications also facilitates the third parties' ability to target advertisements on other computing devices that a patient uses. This is called cross-device targeting.

190. What this means is that third parties, including Facebook and Google, have established a unique identifier for a patient that ties together their desktop, laptop, and smartphone computing devices. Even if a patient has never visited the UH web property on their smartphone, cross-device tracking and marketing is a method through which UH and the third parties work together to target those patients on that device. For example, a patient or potential patient who had visited the UH web property on his desktop, but never on his smartphone, could be targeted with the ad on their smartphone.

191. Cross-device tracking illustrates that the data elements disclosed to the third parties are personally identifiable because they enable the tracking of patients across the multiple devices that the patient owns, even when the patient has never communicated with UH on one or more of their devices.

192. UH has determined that the targeted advertising (including retargeting and cross-device tracking) that is enabled by its disclosure of patient data and communications is of commercial benefit to UH.



193. Upon information and belief, UH obtains additional revenue from its deployment of third-party tracking tools through which it discloses personally identifiable patient data and communications to third parties.

194. Any additional revenue UH obtains from its unauthorized use of its own patients' personally identifiable data and communications is unearned and the rightful property of the patients from whom it was obtained.

195. UH's unauthorized disclosure and use of Plaintiff's and other patients' personally identifiable data and communications is a form of theft, for which the victims are entitled to recover anything acquired with the stolen assets, even if the items acquired have a value that exceeds the value of that which was stolen.

#### **THE VALUE OF THE DATA UH DISCLOSES**

196. The monetization of the data disclosed by UH demonstrates the inherent value of such information.

197. There is an active market for health information which is the subject of significant legal protections under HIPAA and Ohio law. Because of these protections, patient data is not generally known to or readily ascertainable by others who might otherwise obtain economic advantage from its use.

198. The value of the data that companies like Facebook and Google extract is well understood and accepted in the modern economy.

199. Personal information is now viewed as a form of currency and a corporate asset. Professor Paul M. Schwartz has noted in the *Harvard Law Review*:

Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a



corporate asset and have invested heavily in software that facilitates the collection of consumer information.

200. The cash value of Internet users' personal information can be quantified.

201. For example, one 2015 study determined that Americans place more value on their "health condition" than any other piece of data about them, with a minimum value of \$82.90.<sup>13</sup> By comparison, respondents assigned a value of \$67.00 to their passwords, \$55.70 to their Social Security number, and \$40.10 to their credit history.

202. Medical information derived from medical providers garner even more value from its scarcity, which is driven by the fact that it is not legally available to third-party data marketing companies because of strict restrictions on provider disclosures under HIPAA, state laws, and provider standards, including the Hippocratic Oath.

203. Even with strict restrictions on the disclosure of personally identifiable health information, a robust market exists for the trade of de-identified health data.<sup>14</sup>

204. UH's disclosures violate Plaintiff's and other patients' privacy rights not to have their personally identifiable patient data and communications disclosed without their knowledge, authorization, consent, or any further action on their part.

**UH ASSURES PATIENTS THAT IT PROTECTS THEIR PERSONALLY IDENTIFIABLE AND  
NON-PUBLIC MEDICAL INFORMATION**

205. A health care provider must obtain a patient's express written authorization to disclose and use personally identifiable information about patients for marketing purposes.

---

<sup>13</sup> Ponemon Institute, Privacy and Security in a Connected Life: A Study of US Consumers, March 2015, available at <https://www.trendmicro.de/media/report/ponemon-privacy-and-security-in-a-connected-life-us-consumers-report-en.pdf>.

<sup>14</sup> See How Data Brokers Make Money Off Your Medical Records, Scientific American, <https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/>; Your Private Medical Data is for Sale – and It's Driving a Business Worth Billions, The Guardian, <https://www.theguardian.com/technology/2017/jan/10/medical-data-multibillion-dollar-business-report-warns>; The Hidden Global Trade in Patient Medical Data, YaleGlobal Online, <https://yaleglobal.yale.edu/content/hidden-global-trade-patient-medical-data>.



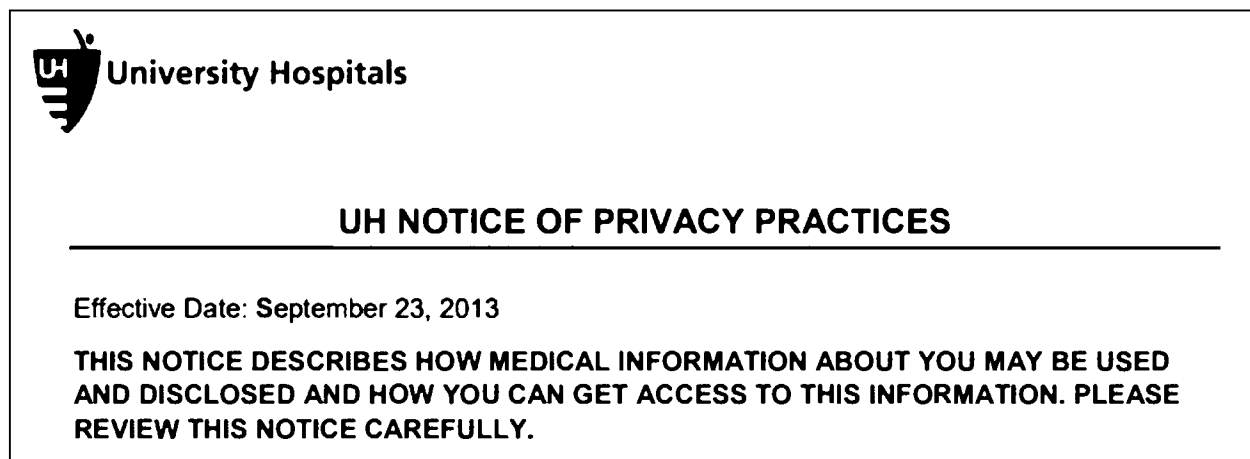
206. Patients who exchange communications with Defendant at [www.uhhospitals.org](http://www.uhhospitals.org) and the UH Patient Portal have a reasonable expectation that their communications will remain confidential.

207. UH does not make any disclosure on its website that would sufficiently alert patients that it discloses, and causes to be transmitted to third parties, patients' personally identifiable data, non-public medical information, and communications.

208. To the contrary, UH's various privacy statements reassure patients that their data is protected and confidential, and give patients the impression that its data practices at [www.uhhospitals.org](http://www.uhhospitals.org) and MyUHCare are "secure."

209. Defendant UH provides patients with a HIPAA Notice of Privacy Practices.

210. UH's HIPAA notice starts with the assertion in bold caps:



211. UH does not disclose anywhere in its HIPAA notice that it deploys source code on its website that commandeers patient computing devices without patient knowledge or authorization to cause those devices to send personally identifiable information and the precise contents of patient communications to third parties.

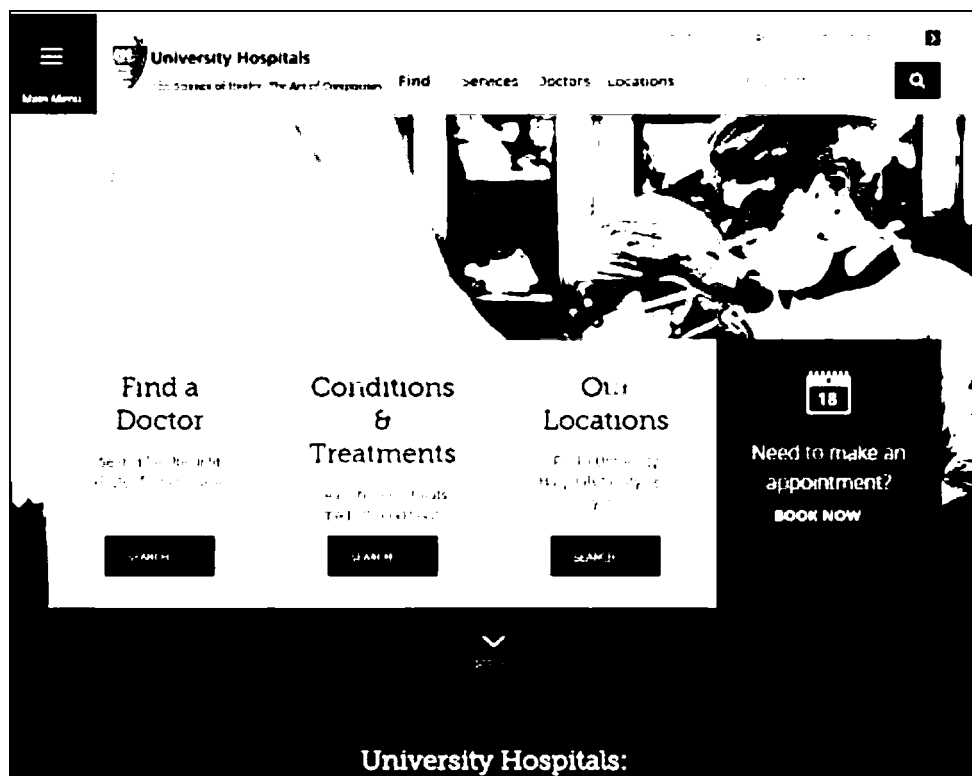
212. UH's HIPAA notice assures patients that "[o]ther uses and disclosures of Medical Information not covered by this Notice or the laws that apply to us will be made only with your



written authorization. For example, ... uses and disclosures of Medical Information for marketing purposes, and disclosures that constitute a sale of Medical Information require your written authorization.”

213. UH also maintains a purported website Privacy Policy that is available via a link in a sub-sub-sub-sub footer on the UHHospitals.org website.

214. The sub-sub-sub-sub footer is not visible unless a patient scrolls down through at least three full screens of material:





View your personal health record, pay your bill, download the UH now app, and more.

**2**

**Figure 1**

2541

☆ 100

### Advanced Mammography Screenings

LHI offers the latest breast cancer screening technology, at 28 locations across Northeast Ohio.

 Springer

**A Trusted Leader  
in Children's  
Health**

UM Rainbow offers the region's largest network of pediatricians, along with advanced specialty care.

... 

### Book Your Own Appointment Online

Making an appointment with a UH doctor has been easier with 24/7 online self scheduling.



Learn about medical education and CME opportunities, how to refer a patient, and other resources for clinicians.



— 2 —

SEE ALL

## Participate in a Clinical Trial

University Hospitals offers over 600 clinical trials including cancer and non-cancer related studies. Use our easy-to-use clinical trials tool to search for a treatment study for you.

100% 

University Hospitals thrives on the generous support of the community, which allows us to advance the personalized care we provide to our patients.

Learn about the opportunities available to the world-class doctors, nurses, health care professionals and support staff who choose to join University Hospitals.

Join our new online panel and tell us what you think about healthcare, your hospital experiences and even television commercials.

2

Back to Top







216. Defendant's Privacy Policy gives patients express assurances that their personally identifiable information is protected.

217. Among other things, Defendant promises the following:

- a. "UH does not sell, trade, or rent personal information about its Site visitors."
- b. "The information we collect about the domain name of the server from which you are visiting is aggregated and used solely to determine the number of visitors to our Site each day, and sources of traffic;"
- c. "We do not respond to any questions concerning specific medical conditions. If you transmit such information, while we will not intentionally release it or make it public, we cannot assure you that the information will be kept private."
- d. "Notwithstanding the foregoing, if you use the 'Schedule Me Now' functionality available through the Site, you will be required to create or use a pre-existing user name and password. Any information collected through the 'Schedule Me Now' functionality will be treated as confidential and subject to University Hospitals HIPAA Notice of Privacy Practices. UH agrees to maintain any information submitted through the 'Schedule Me Now' functionality in compliance with its legal obligations pursuant to all applicable privacy laws, including, without limitation, the Health Insurance Portability and Accountability Act of 1996 ('HIPAA'), as amended from time to time, and its implementing regulations. All other information submitted through the Site may be treated as non-confidential and



nonproprietary as described above and in the Terms & Conditions for the Site.”

218. A health care provider’s duty not to disclose personally identifiable information about patients to third parties for marketing purposes in the absence of the patient’s express authorization is not subject to waiver via an inconspicuous browse-wrap purported privacy policy.

219. A patient’s reasonable expectation that his/her health care provider will not share their information with third parties for marketing purposes, in the absence of their express authorization, is not subject to waiver via an inconspicuous browsewrap purported privacy policy.

220. Browsewrap statements do not constitute enforceable contracts against consumers.

221. The very term “Privacy” policy or statement is deceptive.

222. Consumer surveys consistently show that a majority of Americans falsely believe that the existence of a privacy policy means that “the company keeps confidential all the information it collects on users.”<sup>15</sup>

223. Nevertheless, even if a browsewrap privacy policy could be legally sufficient, Defendant here made express and implied promises of confidentiality in its purported privacy statement that further patient expectations of privacy and assured patients that their personally identifiable data and communications would be kept confidential and secure.

### **CLASS ACTION ALLEGATIONS**

224. Plaintiff brings this class action pursuant to Ohio Civil Rule 23 and seeks certification of the claims on behalf of the following class (the “Class”):

---

<sup>15</sup> Aaron Smith, Half of Americans Don’t Know What a Privacy Policy Is, Pew Research Center (Dec. 4, 2014) (Reporting that more than half of Americans falsely believe, “When a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users.”), available at <https://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/>.



All Ohio residents who are, or were, patients of UH or any of its affiliates, and who used UH's web properties, including, but not limited to, [www.uhhospitals.org](http://www.uhhospitals.org) and the Patient Portal at MyUHCare.

225. Plaintiff reserves the right to redefine the Class prior to certification.

226. This action is properly maintainable as a class action.

227. The Class members are identifiable.

228. Plaintiff is a member of the Class.

229. Defendant is one of the largest health systems in Ohio, performing approximately 10.8 million outpatient procedures annually.<sup>16</sup> The Class for whose benefit this action is brought is so numerous that joinder of all Class members is impracticable.

230. The Class is readily ascertainable and direct notice can be provided from the records maintained by Defendant, or by publication, the cost of which is properly imposed on Defendant.

231. Plaintiff is committed to prosecuting this action and has retained competent counsel experienced in litigation of this nature. Plaintiff's claims are typical of the claims of other Class members and Plaintiff has the same interests as other Class members. Plaintiff has no interests antagonistic to or in conflict with the interests of the other members of the Class. Plaintiff is an adequate representative of the Class and will fairly and adequately protect the interests of the Class.

232. The prosecution of separate actions by individual Class members could create a risk of inconsistent or varying adjudications with respect to individual members of the Class, which could establish incompatible standards of conduct for Defendant or adjudications with respect to individual members of the Class which would, as a practical matter, be dispositive of the interests of the members of the Class not party to the adjudications.

---

<sup>16</sup> <https://www.uhhospitals.org/about-uh>



233. The expense and burden of individual litigation make it impracticable for members of the Class to redress the wrongs done to them individually. If a class action is not permitted, Class members will continue to suffer losses and Defendant's misconduct will continue without proper remedy.

234. Plaintiff's claims arise from a practice which Defendant applies uniformly to all the similarly situated Class members and are based on the same legal theories as all other members of the putative class. Defendant has acted and refused to act on grounds generally applicable to the entire Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

235. Plaintiff anticipates no unusual difficulties in the management of this litigation as a class action.

236. For the above reasons, a class action is superior to other available methods for the fair and efficient adjudication of this action.

237. Because Defendant's conduct was and is uniform as to all Class members, the material elements of Plaintiff's claims and those of absent Class members are subject to common proof, and the outcome of Plaintiff's individual actions will be dispositive for the Class. Indeed, there are questions of law and fact common to Class members that predominate over any questions affecting only individual members of the Class. A class action will generate common answers to the below questions, which are apt to drive resolution:

- a. Whether Defendant's practices relating to its disclosures of the Class communications with Defendant to third-party companies attached to personal information was intentional;
- b. Whether Defendant's practices relating to its disclosures of the Class communications with Defendant to third-party companies attached to personally identifiable information constituted a breach of provider-patient confidentiality;



- c. Whether this case may be maintained as a class action;
- d. Whether and to what extent Class members are entitled to damages and other monetary relief;
- e. Whether and to what extent Class members are entitled to equitable relief including, but not limited to, a preliminary and/or permanent injunction; and
- f. Whether and to what extent Class members are entitled to attorneys' fees and costs.

**COUNT I – DISCLOSURE NON-PUBLIC MEDICAL INFORMATION PURSUANT TO  
*BIDDLE V. WARREN GEN. HOSP.*, 86 OHIO ST.3D 395 (1999)**

238. Plaintiff incorporates all prior paragraphs as if fully stated herein.

239. In Ohio, medical providers have an obligation to their patients to keep non-public medical information completely confidential.

240. Disclosure of confidential medical information by a medical provider in Ohio without consent results in civil liability.

241. Plaintiff is a patient of UH.

242. Plaintiff has reasonable expectations of privacy in her communications exchanged with UH, including communications exchanged at [www.uhhospitals.org](http://www.uhhospitals.org) on the log-in page for the UH Patient Portal, and within the MyUHCare patient portal.

243. Plaintiff's reasonable expectations of privacy in the communications exchanged with UH were further buttressed by UH's express promises including, but not limited to, "[o]ther uses and disclosures of Medical Information not covered by this Notice or the laws that apply to us will be made only with your written authorization. For example, ... uses and disclosures of Medical Information for marketing purposes, and disclosures that constitute a sale of Medical Information require your written authorization."

244. Contrary to its obligations as a provider and its express promises of confidentiality, UH deployed source code to disclose and transmit Plaintiff's personally identifiable, non-public



medical information, and the contents of their communications exchanged with UH to numerous third parties.

245. The third-party recipients to whom UH disclosed Plaintiff's personally identifiable, non-public medical information, and communications include Facebook, Google, Microsoft (Bing), Invoca.net, Liveperson.net, LPSNMedia.net, and Typekit.net.

246. UH's disclosures of Plaintiff's personally identifiable, non-public medical information, and the contents of their communications with UH were made without her knowledge, consent, or authorization, and were unprivileged.

247. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the health care provider and the patient.

248. As a direct and proximate cause of UH's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Defendant caused Plaintiff and other patients the following damages:

- a. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private;
- b. UH eroded the essential confidential nature of the provider-patient relationship;
- c. General Damages for invasion of their rights in an amount to be determined by a jury;
- d. Nominal Damages for each independent violation;
- e. UH took something of value from Plaintiff and Class members and derived benefit therefrom without Plaintiff's and Class members' knowledge or informed consent and without compensating Plaintiff for the data;
- f. Plaintiff and Class members did not get the full value of the medical services for which they paid, which included UH's duty to maintain confidentiality;
- g. UH's actions diminished the value of Plaintiff's and Class members' personal information; and



- h. UH's actions violated the property rights Plaintiff and Class members have in their personally identifiable medical information and the content of their communications.

## **COUNT II – BREACH OF CONFIDENCE**

249. Plaintiff incorporates all prior paragraphs as if fully stated herein.

250. In Ohio, medical providers have a duty to their patients to keep non-public medical information completely confidential.

251. Disclosure of confidential medical information by a medical provider in Ohio without consent results in civil liability.

252. Plaintiff is a patient of UH.

253. Plaintiff has reasonable expectations of privacy in her communications exchanged with UH, including communications exchanged at [www.uhhospitals.org](http://www.uhhospitals.org) on the log-in page for the UH Patient Portal, and within the MyUHCare patient portal.

254. Plaintiff's reasonable expectations of privacy in the communications exchanged with UH were further buttressed by UH's express promises including, but not limited to, "[o]ther uses and disclosures of Medical Information not covered by this Notice or the laws that apply to us will be made only with your written authorization. For example, ... uses and disclosures of Medical Information for marketing purposes, and disclosures that constitute a sale of Medical Information require your written authorization."

255. Contrary to its duties as a medical provider and its express promises of confidentiality, UH deployed source code to disclose and transmit Plaintiff's personally identifiable, non-public medical information, and the contents of their communications exchanged with UH to numerous third parties.



256. The third-party recipients to whom UH disclosed Plaintiff's personally identifiable, non-public medical information, and communications include Facebook, Google, Microsoft (Bing), Invoca.net, Liveperson.net, LPSNMedia.net, and Typekit.net.

257. UH's disclosures of Plaintiff's personally identifiable, non-public medical information, and the contents of their communications with UH were made without his knowledge, consent, or authorization, and were unprivileged.

258. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the health care provider and the patient.

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

- a. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private;
- b. UH eroded the essential confidential nature of the provider-patient relationship;
- c. General Damages for invasion of their rights in an amount to be determined by a jury;
- d. Nominal Damages for each independent violation;
- e. UH took something of value from Plaintiff and Class members and derived benefit therefrom without Plaintiff's and Class members' knowledge or informed consent and without compensating Plaintiff for the data;
- f. Plaintiff and Class members did not get the full value of the medical services for which they paid, which included UH's duty to maintain confidentiality;
- g. UH's actions diminished the value of Plaintiff's and Class members' personal information; and
- h. UH's actions violated the property rights Plaintiff and Class members have in their personally identifiable medical information and the content of their communications.



### **COUNT III – INVASION OF PRIVACY – INTRUSION UPON SECLUSION**

260. Plaintiff re-states all previous allegations as if stated fully herein.

261. Plaintiff and Class members have objectively reasonable expectation of solitude or seclusion in their personal and private information and the confidentiality of the content of their communications with their medical provider.

262. UH intruded upon that seclusion by deploying source code at its web properties that caused Plaintiff and other patient Class members' private information and communications to be disclosed to third parties for marketing purposes without patient knowledge, authorization, consent, notice, or privilege.

263. UH's actions of disclosing its own patients' private information and the content of communications that patients exchanged with UH under reasonable expectations of privacy and UH's express promise to maintain confidentiality would be highly offensive to a reasonable person.

264. UH's breach caused Plaintiff and other patients the following damages:

- a. Confidential information that Plaintiff and Class members intended to remain private is no more, the highly offensive breach of which entitles Plaintiff and other patients to General Damages for the tort of intrusion upon seclusion;
- b. UH took something of value from Plaintiff's and Class members and derived benefit therefrom without Plaintiff's and Class members' knowledge or informed consent and without sharing the benefit of such value;
- c. Plaintiff and Class members did not get the full value of the medical services for which they paid, *i.e.*, benefit of the bargain, which included UH's duty to maintain confidentiality; and



- d. UH eroded the essential confidential nature of the provider-patient relationship.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, asked for judgment in their favor, and that the Court award:

- a. General Damages for the violation of privacy in an amount to be determined by a jury without reference to specific harm;
- b. A reasonable royalty for UH's misappropriation of personally identifiable, non-public medical information, and communications;
- c. Imposition of a constructive trust against UH through which Plaintiff can be compensated for any unjust enrichment gained by UH;
- d. The value of the data UH disclosed and used without Plaintiff's and other patients' authorization;
- e. Attorneys' fees and litigation costs reasonably expended; and
- f. Punitive damages in an amount to be determined by a jury.

In addition, Plaintiff, on behalf of herself and all others similarly situated, respectfully request this Court enter an order for equitable relief, enjoining UH from making any further disclosures of Plaintiff's or Class members' communications with UH.



**DEMAND FOR JURY TRIAL**

Plaintiff hereby makes a demand for trial by jury on all issues so triable.

Respectfully submitted,

/s/ Stuart E. Scott

Stuart E. Scott (0064834)

Kevin C. Hulick (0093921)

**SPANGENBERG SHIBLEY & LIBER LLP**

1001 Lakeside Avenue East, Suite 1700

Cleveland, OH 44114

(216) 696-3232

(216) 696-3924 (FAX)

sscott@spanglaw.com

khulick@spanglaw.com

Mitchell Breit (*pro hac vice* to be submitted)

Jason 'Jay' Barnes (*pro hac vice* to be submitted)

**SIMMONS HANLY CONROY LLC**

112 Madison Avenue, 7th Floor

New York, NY 10016-7416

(212) 784-6400

(212) 213-5949 (FAX)

mbreit@simmonsfirm.com

jaybarnes@simmonsfirm.com

*Counsel for Plaintiff and the Proposed Class*