IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

MARGUERITE KUROWSKI and BRENDA MCCLENDON, on behalf of themselves and all others similarly situated, *Plaintiffs*, v. RUSH SYSTEM FOR HEALTH d/b/a RUSH UNIVERSITY SYSTEM FOR HEALTH, *Defendant*.	Case No. _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Marguerite Kurowski ("Kurowski") and Brenda McClendon ("McClendon") (collectively "Plaintiffs"), on behalf of themselves and all others similarly situated, upon personal knowledge as to Plaintiffs' own conduct and on information and belief as to all other matters based upon investigation of counsel, such that each allegation has evidentiary support or is likely to have evidentiary support upon further investigation and discovery, and for their Class Action Complaint against Defendant Rush System for Health d/b/a Rush University System for Health ("Rush" or "Defendant"), states as follows:

NATURE OF THE ACTION

1. Medical providers have a duty to patients to keep patient data, communications, diagnoses, and treatment information completely confidential unless authorized to make disclosures by the patient.

2. Patients are aware of and must be able to rely upon the protections, obligations, and expectations provided by statutory, regulatory, and common law as well as the promises of confidentiality contained within the Hippocratic Oath.

3. A patient who exchanges communications with Rush has a reasonable expectation of privacy that their personally identifiable data and the content of their communications will not be intercepted, transmitted, re-directed, or disclosed by Rush to third parties without the patient's knowledge, consent, action or authorization.

4. Rush nonetheless discloses Plaintiffs' and Class members' personally identifiable patient data, including their status as patients and the contents of their communications with Rush, to third parties including Facebook, Google, and a digital advertising company called "Bidtellect."

5. Despite its ethical and legal obligations and its patients' reasonable expectations of privacy, Rush systematically violated the medical privacy rights of its patients by causing the contemporaneous unauthorized interception and transmission of personally identifiable patient data, and re-direction and disclosure of the precise content of patient communications with Rush to third parties including Facebook, Google, and Bidtellect without patient knowledge, consent, authorization, or any affirmative action.

6. Rush's conduct gives rise to at least five causes of action: (1) violation of § 2511 of the ECPA; (2) breach of implied duty of confidentiality; (3) violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq*.; (4) violations of the Illinois Deceptive Trade Practices Act, 815 ILCS 510/1 *et seq*; and (5) invasion of privacy - intrusion upon seclusion.

7. As a result of Rush's conduct in disclosing personally identifiable patient data and re-directing and disclosing the content of patient communications to third parties without patient knowledge, consent, authorization, or any further action by the patient, Rush has caused damage to Plaintiffs and other patient Class Members in that:

a. Sensitive and confidential information that Plaintiffs and patient Class members intended to remain private is no longer private;

b. Defendant eroded the essential confidential nature of the provider-patient relationship;

c. Defendant took something of value, to wit: personal data, from Plaintiffs and patient Class members and derived benefit therefrom without Plaintiffs and Class members' knowledge or informed consent or authorization and without sharing the benefit of such value;

d. Plaintiffs and other patient Class members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

e. Defendant's actions diminished the value of Plaintiffs and Class members' personal information.

PARTIES TO THE ACTION

8. Plaintiff Marguerite Kurowski is a resident of Will County, Illinois, a Rush patient, and MyChart patient portal user. Kurowski has been a Rush patient since approximately 2017 and has been a MyChart patient portal user since 2017.

9. Plaintiff Brenda McClendon is a resident of Cook County, Illinois, a Rush patient and MyChart patient portal user. McClendon has been a Rush patient since approximately 1999 and has been a MyChart patient portal user since 2017.

10. Defendant Rush System for Health d/b/a Rush University System for Health is an Illinois non-profit corporation headquartered in Chicago, Illinois. Rush encourages patients to use, and communicates with patients through the Rush web properties, including the MyChart patient

portal. Rush University Medical Center, Rush Copley Medical Center, and Rush Oak Park Hospital are all part of Rush.

JURISDICTION AND VENUE

11. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332, because: (a) this is a proposed class action in which there are at least 100 Class members; (b) the parties are minimally diverse, as at least one member of the proposed Patient Class is domiciled in a different state than Defendant; and (c) the combined claims of Class members exceed $5,000,000, exclusive of interest, attorneys' fees, and costs.

12. This Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1331 because the action arises under the laws of the United States, specifically, 18 U.S.C. § 2511, of the Electronic Communications Privacy Act ("ECPA").

13. This Court additionally has supplemental jurisdiction over Plaintiffs' state law claims under 28 U.S.C. § 1367(a), because they are so related to Plaintiffs' federal claims that they form part of the same case or controversy under Article III of the United States Constitution.

14. This Court has personal jurisdiction over Rush because Rush regularly conducts business throughout northern Illinois.

15. Venue is also appropriate in this District under 28 U.S.C. § 1391(b)(2) because, a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this district.

FACTUAL ALLEGATIONS

Patients Have Reasonable Expectations of Privacy

16. Rush maintains various web-properties, including www.rush.edu and mychart.rush.edu, for its patients to communicate with Rush, including but not limited to exchanging communications about bill payment, doctors, services, treatments, conditions, appointments, and access to an online MyChart patient portal.

17. Rush actively encourages patients to use its web properties, including the MyChart patient portal.

18. Plaintiffs are patients of Rush and users of the MyChart patient portal.

19. As Rush patients, Plaintiffs have a reasonable expectation of privacy that Rush, their health care provider, and its business associates, including Epic Software Systems, will not disclose their personally identifiable information or the content of their communications to third parties without their express authorization.

20. Plaintiffs' and other Rush patients' reasonable expectations of privacy in their personally identifiable data and communications exchanged with Rush are derived from several sources, including:

a. Rush's status as Plaintiffs' and other patients' health care provider;

b. Rush's common law obligation to maintain the confidentiality of patient data and communications;

c. State and federal laws and regulations protecting the confidentiality of medical information;

d. State and federal laws protecting the confidentiality of communications and computer data;

e. State laws protecting unauthorized use of personal means of identification;

f. Defendant's express promises of confidentiality; and

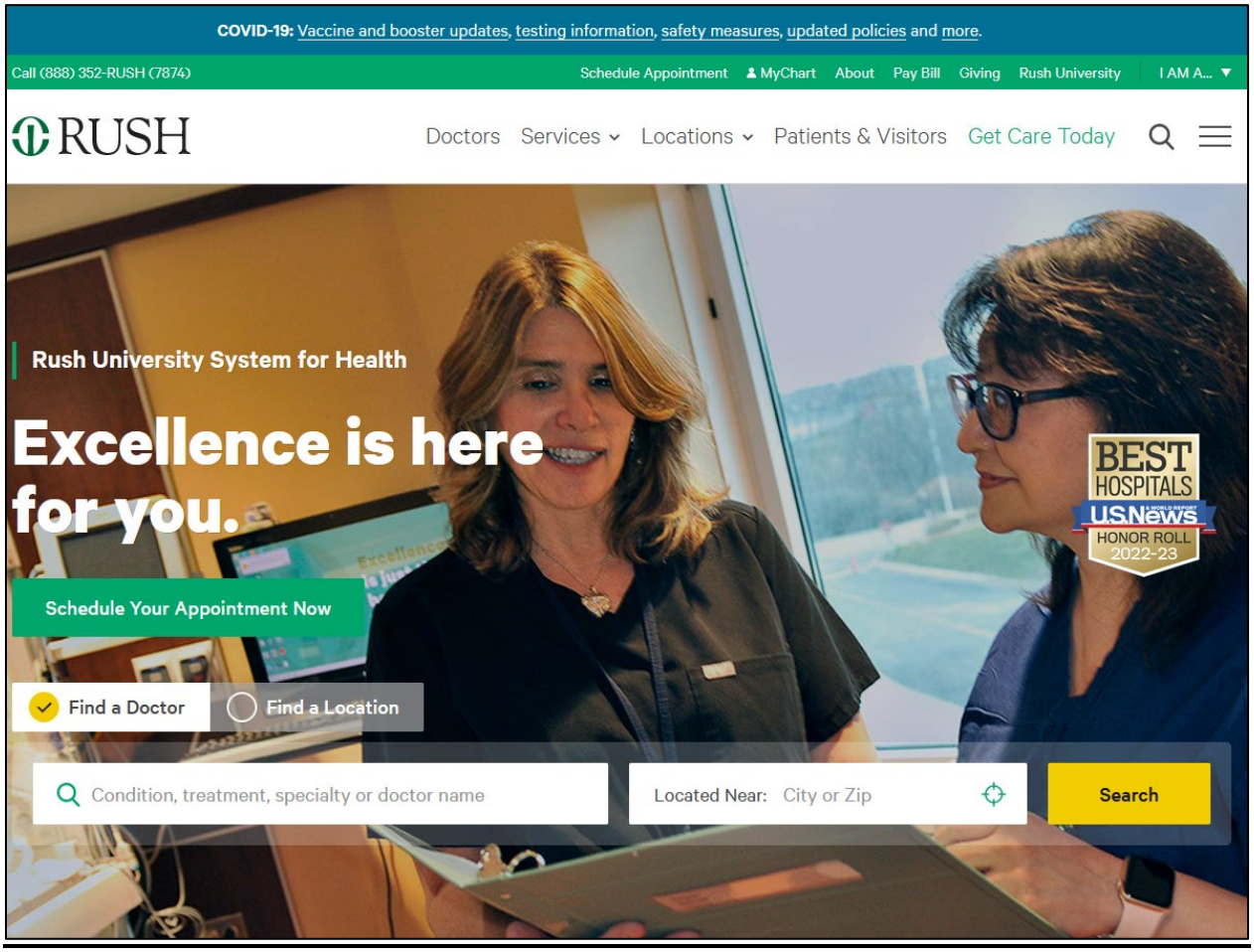
g. Defendant's implied promises of confidentiality.

The Rush Web-Property

21. Plaintiffs interacted with Rush's web properties, including using the website to create an account on Rush's MyChart patient portal.

22. Plaintiffs exchanged communications with Rush via the Rush web property, including using Rush's MyChart patient portal, identifying themselves to Rush as a patient, and exchanging communications relating to their particular providers and medical conditions.

23. Rush's homepage shows how the web property is designed for use by patients. The homepage provides patients with tools to "Find a Doctor," "Find a Location," search for "Condition, treatment, specialty or doctor name," "Schedule Appointment," Pay Bill," and access the "MyChart" patient portal:



The MyChart Patient Portal

24. Rush also maintains a patient portal, mychart.rush.edu, for its patients to communicate with Rush, with options including but not limited to "communicate with your care team," "access your test results," and "manage your appointments."

25. Rush uses the "MyChart" website and mobile application to allow patients to access the MyChart patient portal, which is a software system designed and licensed to Rush by Epic Software Systems ("Epic").

26. Epic is a privately owned health care software company that provides services to 250 million patients, including two thirds of the US population.

27. Epic is a "developer-led" company that builds its software systems "in-house."[1]

28. Epic states its software "offers patients personalized and secure online access to portions of their medical records" and "enables you to securely use the Internet to help manage and receive information about your health. With MyChart, you can:

- Request medical appointments.
- View your health summary.
- View test results.
- Request prescription renewals.
- Access trusted health information resources.
- Communicate electronically and securely with your medical care team."[2]

29. Despite these promises, Epic's MyChart software system was designed to permit licensees—such as Rush—to deploy "custom analytics scripts" within MyChart including, for example, Google Analytics, which allows for the transmission of patients' personally identifiable

[1] *About Us,* Epic, https://www.epic.com/about (last visited July 15, 2022).
[2] https://mychart.rush.edu/mychart/Authentication/Login?

information, including medical and health-related information, and communications to third parties.[3]

30. Rush took advantage of MyChart's analytics compatibility by knowingly and secretly deploying Google source code throughout its web properties, including inside the MyChart patient portal, that causes the contemporaneous unauthorized transmission of personally identifiable patient data and re-direction of the precise content of patient communications with Rush to be sent to Google whenever a Rush patient uses the Rush web properties, including the MyChart patient portal.

31. Like its other web properties, Rush actively encourages patients to use the MyChart patient portal.

32. As Rush patients and MyChart patient portal users, Plaintiffs exchanged communications with Rush through its web properties, including through the MyChart patient portal, each time Plaintiffs used the MyChart patient portal or other Rush web properties. Rush caused the contemporaneous unauthorized transmission of Plaintiffs' personally identifiable patient data and re-direction of the precise content of Plaintiffs' patient communications with Rush to be sent to Google whenever Plaintiffs used the Rush web properties, including the MyChart patient portal.

The Forms of Patient Personally Identifiable Information That Rush Causes to Be Transmitted to Third-Party Marketing Companies

33. Despite its own legal obligations and internal policies, Rush's source code causes the interception and transmission of the following personally identifiable information ("PII") to

[3] Feathers, T., *Pixel Hunt: Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, The Markup (June 16, 2022) (available at https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites).

third parties whenever a patient uses Rush's web properties, including www.rush.edu and the MyChart patient portal:

a. Patient IP addresses;

b. Unique, persistent patient cookie identifiers;

c. Device identifiers;

d. Account numbers;

e. URLs;

f. Other unique identifying numbers, characteristics, or codes; and

g. Browser-fingerprints.

34. Whenever a patient uses Rush's web properties, including www.rush.edu and the MyChart patient portal, Rush intercepts, causes transmission of, and uses personally identifiable patient data without patient knowledge, consent, authorization, or any further action by the patient.

35. Despite its legal obligations, Rush's source code causes the interception and transmission of the precise content of patients' communications with Rush to third parties.

36. Rush discloses Plaintiffs' and Class members' personally identifiable patient data, including their status as patients and the contents of their communications with Defendant, to third parties including Facebook, Google, and Bidtellect.

37. Rush's unauthorized disclosures to third parties includes information that identifies Plaintiffs and Class members as Rush patients and aids the third-parties in receiving and recording patient communications pertaining to or about specific doctors, conditions, treatments, payments, and connections to the MyChart patient portal.

38. Rush's third-party disclosures occur because Rush intentionally deploys source code at www.rush.edu and www.mychart.rush.edu that commandeers patients' web-browsers and

causes personally identifiable patient data, as well as the exact contents of communications exchanged between Defendant and their patients, to be sent to third parties.

39. Rush's third-party disclosures occur contemporaneous to communications with Plaintiff and Class members.

40. By design, the third-parties receive and record the exact contents of these communications before the full response from Rush to Plaintiffs or a Class member has been rendered on the screen of the patient's device and while the communication between Rush and patients remains ongoing.

41. Rush is not required to make disclosures to Facebook, Google, or Bidtellect for Rush's websites or services to function.

42. Rush causes transmission and disclosure of the precise content of patients' communications with Rush to third parties without patient knowledge, consent, authorization, or any further action by the patient.

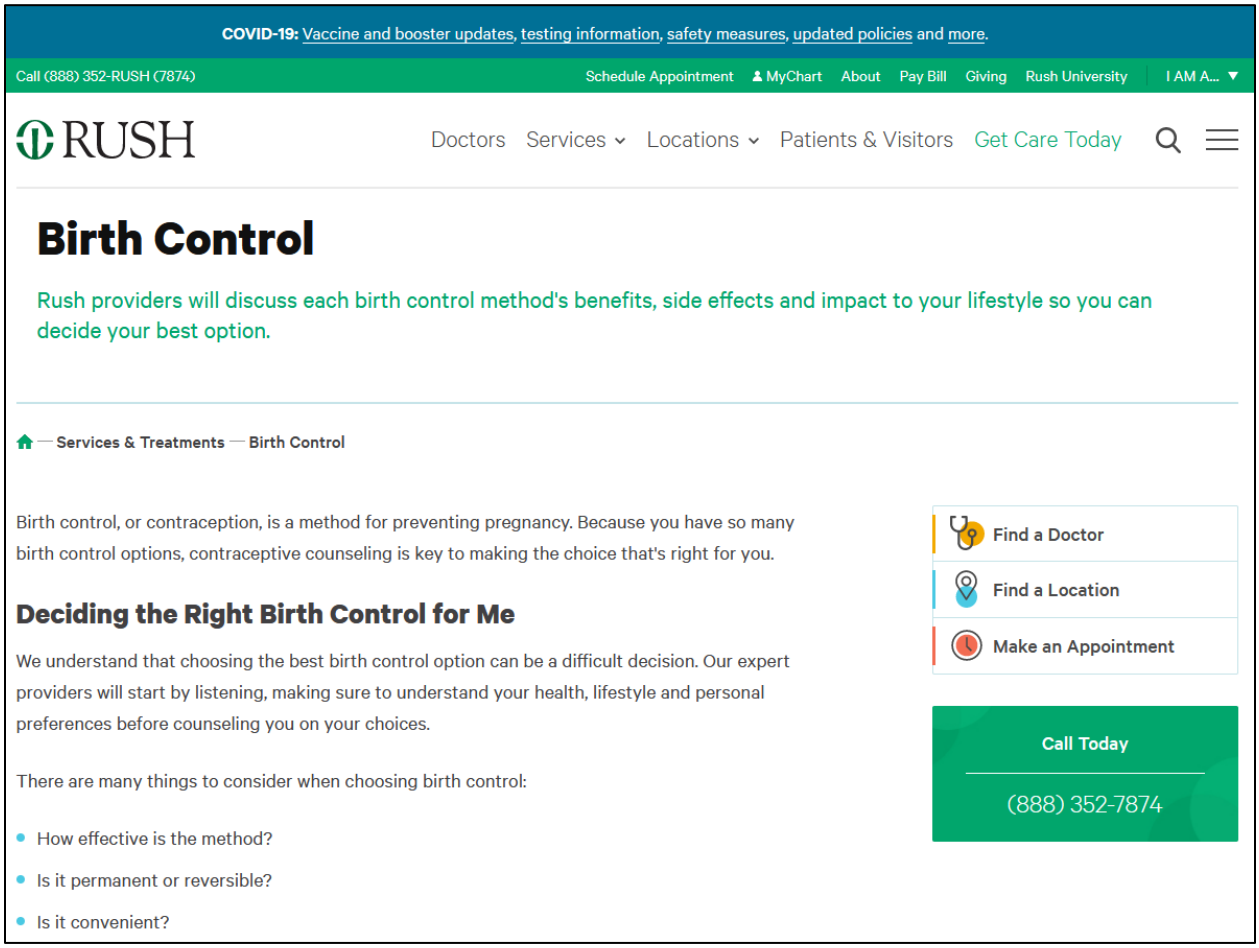
Rush Secretly Transmits Personally Identifiable Patient Data and Re-Directs the Content of Patient Communications to Third Parties

43. Web browsers are software applications that allow consumer to exchange electronic communications over the Internet.

44. 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.

45. The basic command web browsers use to communicate with website servers is called a GET request. As an example of how Rush uses GET requests to communicate, when a patient types in a Rush webpage such as https://www.rush.edu/treatments/birth-control into the navigation bar of her web-browser (or, just as, if not more frequently, takes the technological shortcut of clicking a preset hyperlink to the page), the patient's web-browser makes connection

with the server for Rush and sends the following: "GET /treatments/birth-control HTTP/1.1" and the following webpage loads on the patient's browser:



46. 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.

47. In response to receiving a GET or POST request, the server for the entity with which the user is exchanging communications, in this case Rush's server, will send a set of instructions to the web-browser, commanding the browser with source code that (1) directs the browser on how to render the entity's response and, in many circumstances, (2) commands the browser to transmit

personally identifiable data about the Internet user and re-direct the precise content of the user's GET or POST requests to various third parties.

48. In addition to these communications between Rush and the patient, however, when a patient communicates with Rush's website (whether by typing in a webpage, putting in a search, clicking on a hyperlink, or otherwise), Rush also causes some of that information to be transmitted to third parties without the patient's knowledge or authorization. The third parties to whom user data is transmitted and the content of communications redirected are typically procured by websites to track users' personally identifiable data and communications for marketing purposes, i.e. targeted advertising.

49. In many such cases, the third parties acquire the content of user communications through a 1x1 pixel (the smallest dot on a user's screen) called a web bug, tracking pixel, or web beacon. These web-bugs are tiny and purposefully camouflaged to remain invisible to the user.

50. Web bugs can be placed directly on a page by a web developer or can be funneled through a "tag manager" service to make the invisible tracking run more efficiently and to further obscure the third parties to whom the website transmits personally identifiable user data and re-directs the content of communications.

51. 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 seek to transmit and re-direct user data and communications. On websites with several third-party trackers, this may cause the page to load more slowly and increases risk of a coding error, effecting functionality and usability. A "tag manager" offers the website developer a container in which to place all third-party source code. Instead of placing all

third-party source code directly on the webpage, the developer places the source code within its account at the tag manager.

52. Google explains the benefits of Google Tag Manager in an Introduction to Google Tag Manager video on YouTube. [4] 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.
>
> 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.

53. Rush deploys Google Tag Manager on its websites through an "iframe," a nested "frame" that exists within the Rush web property that is, in reality, an invisible window through which Rush funnels web bugs for third parties to secretly acquire the content of patient communications without any knowledge, consent, authorization, or further action of patients.

54. Rush's Google Tag Manager source code is designed to be invisible. For example, on the "birth control" communications page set forth above, the GTM source code used by Rush specifies an "iframe" with a height of 0, width of 0, display of none, and visibility of hidden.

[4] See https://www.youtube.com/watch?v=KRvbFpeZ11Y, audio from 0:04 to 1:40.

55. Rush then funnels invisible 1x1 web bugs or pixels through this purposefully invisible iframe to help third-parties track, acquire, and record patient data and communications.

56. By design, none of the tracking is visible to patients at the Rush web properties.

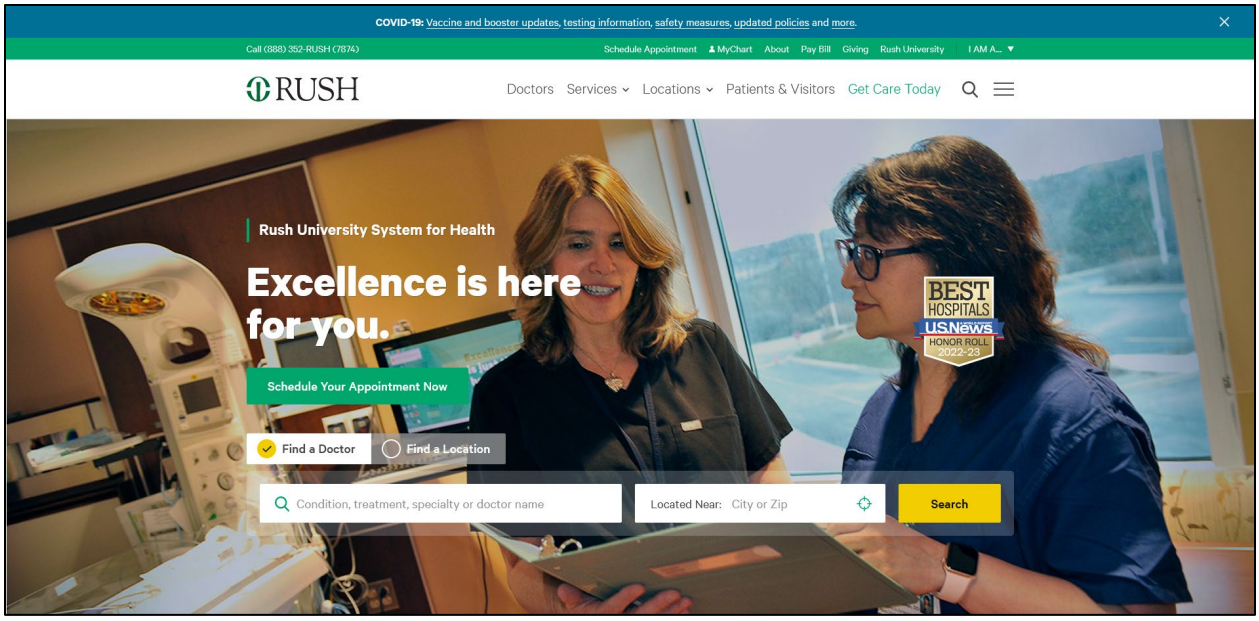
57. For example, the reproductive medicine page above does not include anything to apprise patients that Rush is causing their personally identifiable data to be transmitted and the content of their communications re-directed to third parties including Facebook and Google.

What Happens When a Patient Communicates with Rush at Rush's Web Properties

58. "Fiddler" is a commercially available software application used by web developers to test how their various applications and source codes operate. By using Fiddler, one can also capture and record communications and other data transmissions that flow to and from a web-browser over the Internet. The following is derived from a test Fiddler analysis in connection with the www.rush.edu web property.

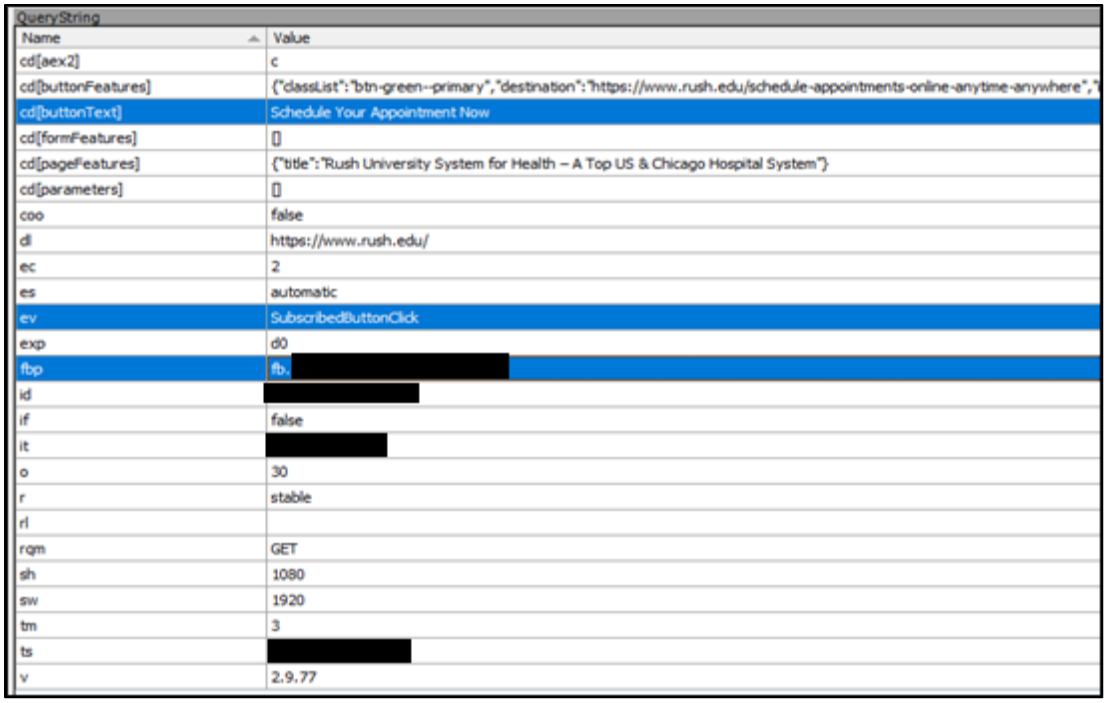
59. When a patient first visits the www.rush.edu homepage, the source code that Rush utilizes causes personally identifiable patient data to be transmitted and the contents of patient communications to be re-direct to third parties connected to the fact that the patient is present at the Rush property.

60. Many of the tabs provided by Rush on its web properties are specific to patients—i.e. "Schedule Your Appointment Now," "Pay Your Bill," "Medical Records," "Connect With Rush," and "Plan Your Stay," among others (collectively "Patient Tabs"). Clicking on any of of the Patient Tabs identifies the person using the web property as a patient for purposes of using the Rush web property:



61. When a patient clicks the tab to "Schedule Your Appointment Now," Rush causes the transmission of the patient's personally identifiable data and re-directs the content of the patient's click of the "Schedule Your Appointment Now" button to Facebook.

62. For example, Fiddler shows the following types of data are transmitted to Facebook through a test "formPOST" request caused by Rush's source code whenever a patient clicks on the Schedule Your Appointment Now link:



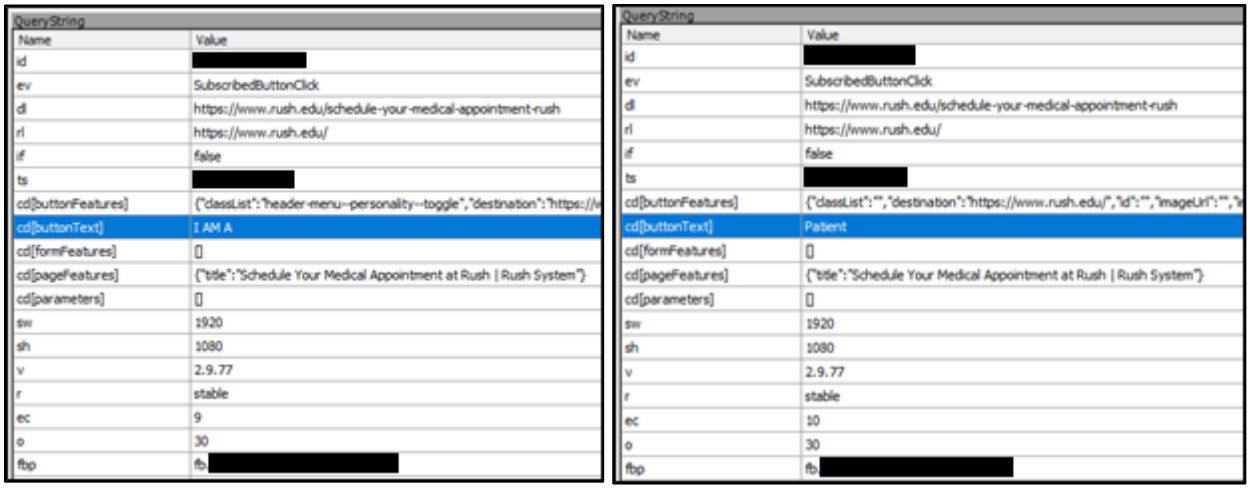
QueryString

Name	Value
cd[aex2]	c
cd[buttonFeatures]	{"classList":"btn-green--primary","destination":"https://www.rush.edu/schedule-appointments-online-anytime-anywhere","t
cd[buttonText]	Schedule Your Appointment Now
cd[formFeatures]	[]
cd[pageFeatures]	{"title":"Rush University System for Health – A Top US & Chicago Hospital System"}
cd[parameters]	[]
coo	false
dl	https://www.rush.edu/
ec	2
es	automatic
ev	SubscribedButtonClick
exp	d0
fbp	fb. [redacted]
id	[redacted]
if	false
it	[redacted]
o	30
r	stable
rl	
rqm	GET
sh	1080
sw	1920
tm	3
ts	[redacted]
v	2.9.77

This chart shows disclosure to Facebook that the patient engaged in an event ('ev') labeled "SubscribedButtonClick," that the "buttonText" was "Schedule Your Appointment Now," that the button was clicked from https://www.rush.edu, and the details of the first-party fbp cookie assigned by Rush.

63. Rush causes multiple data transmissions containing personally identifiable patient information to be made to Facebook before the data is sent to Rush.

64. Rush does not just disclose patient status to Facebook implicitly through the transmission of MyChart-related activity, but directly by transmitting the text "I AM A … Patient" to Facebook in successive transmissions:



QueryString

Name	Value
id	[redacted]
ev	SubscribedButtonClick
dl	https://www.rush.edu/schedule-your-medical-appointment-rush
rl	https://www.rush.edu/
if	false
ts	[redacted]
cd[buttonFeatures]	{"classList":"header-menu--personality--toggle","destination":"https://w
cd[buttonText]	I AM A
cd[formFeatures]	[]
cd[pageFeatures]	{"title":"Schedule Your Medical Appointment at Rush | Rush System"}
cd[parameters]	[]
sw	1920
sh	1080
v	2.9.77
r	stable
ec	9
o	30
fbp	fb[redacted]

QueryString

Name	Value
id	[redacted]
ev	SubscribedButtonClick
dl	https://www.rush.edu/schedule-your-medical-appointment-rush
rl	https://www.rush.edu/
if	false
ts	[redacted]
cd[buttonFeatures]	{"classList":"","destination":"https://www.rush.edu/","id":"","imageUrl":"","w
cd[buttonText]	Patient
cd[formFeatures]	[]
cd[pageFeatures]	{"title":"Schedule Your Medical Appointment at Rush | Rush System"}
cd[parameters]	[]
sw	1920
sh	1080
v	2.9.77
r	stable
ec	10
o	30
fbp	fb[redacted]

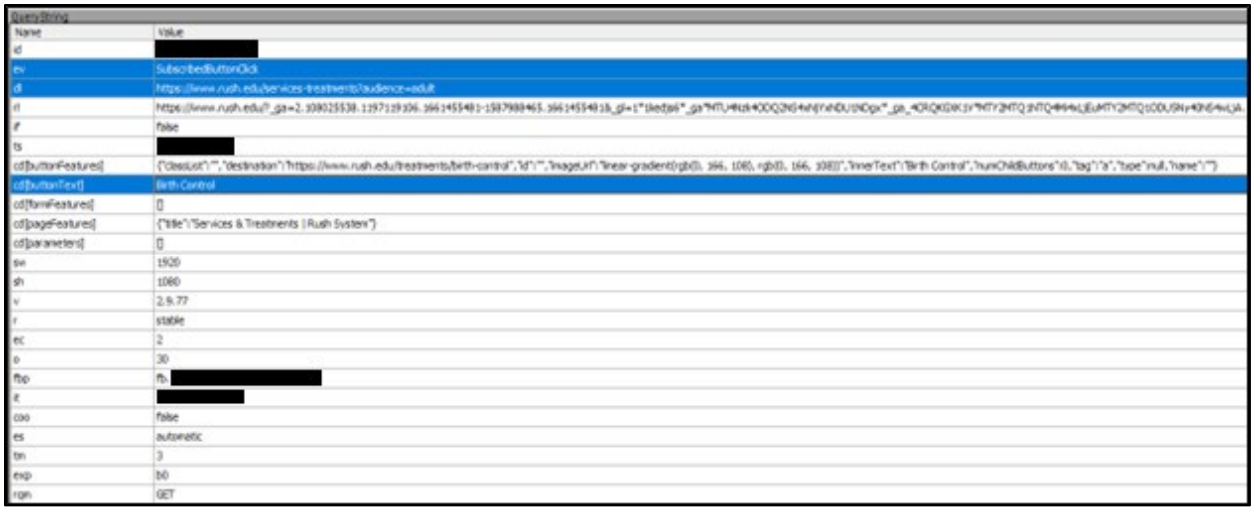
65. Rush causes similar data transmissions to be sent to Facebook with every communication that a patient sends using the Patient Tabs.

66. Rush also causes similar data transmissions to be sent to Facebook with every communication that a patient sends at its www.rush.edu web property generally.

67. For example, when a patient sends a communication searching for more information on "birth control" (or any other search), Rush causes data transmissions to be made to third parties, including Facebook, Google, and Bidtellect, that include personally identifiable patient data and the content of the patient's re-directed communication.

68. Immediately upon a patient sending the "birth control" communication to Rush, the source code triggers separate contemporaneous data transmissions containing personally identifiable patient data and the content of the patient's communication to third parties, including Facebook, Google, and Bidtellect.

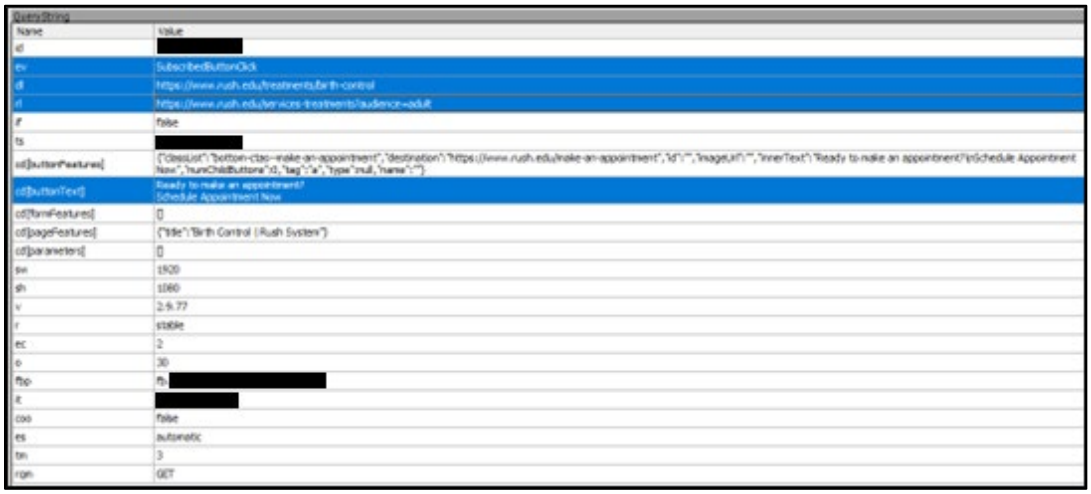
69. An example transmission to Facebook includes the following:



Name	Value
id	[redacted]
ev	SubscribedButtonClick
dl	https://www.rush.edu/services-treatments?audience=adult
rl	https://www.rush.edu/?_ga=2.108025538.1297129306.1661455481-1587988465.1661455481&_gl=1*1ke6je6*_ga*NTU4Nzk4ODQ2NS4xNjYxNDU0NDgx*_ga_4DRQKDDKJY*MTY2MTQ3NTQ4Mi4yLjEuMTY2MTQ1ODU5Ny4wNS4wLjA.
if	false
ts	[redacted]
cd[buttonFeatures]	{"classList":"","destination":"https://www.rush.edu/treatments/birth-control","id":"","imageUrl":"linear-gradient(rgb(0, 166, 108), rgb(0, 166, 108))","innerText":"Birth Control","numChildButtons":0,"tag":"a","type":null,"name":""}
cd[buttonText]	Birth Control
cd[formFeatures]	[]
cd[pageFeatures]	{"title":"Services & Treatments | Rush System"}
cd[parameters]	[]
sw	1920
sh	1080
v	2.9.77
r	stable
ec	2
o	30
fbp	fb.[redacted]
it	[redacted]
coo	false
es	automatic
tm	3
exp	b0
rqm	GET

This shows that the patient has engaged in a "SubscribedButtonClick," that the text of the button was "Birth Control," that the patient sending the request was an adult (*i.e.* audience=adult), the patient's Google Analytics identifier, and the patient's Facebook Pixel identifier.

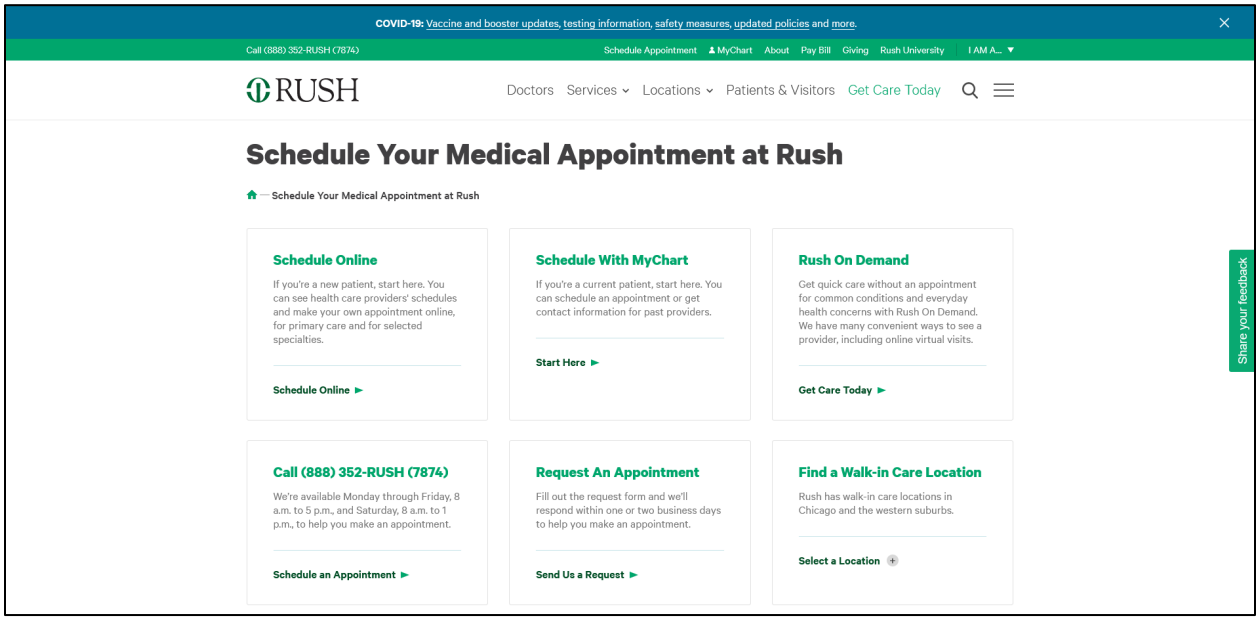
70. If the patient continues his or her browsing session to schedule an appointment, Rush transmits the appointment request to Facebook:



Name	Value
id	[redacted]
ev	SubscribedButtonClick
dl	https://www.rush.edu/treatments/birth-control
rl	https://www.rush.edu/services-treatments?audience=adult
if	false
ts	[redacted]
cd[buttonFeatures]	{"classList":"button-cta--make-an-appointment","destination":"https://www.rush.edu/make-an-appointment","id":"","imageUrl":"","innerText":"Ready to make an appointment?\nSchedule Appointment Now","numChildButtons":0,"tag":"a","type":null,"name":""}
cd[buttonText]	Ready to make an appointment? Schedule Appointment Now
cd[formFeatures]	[]
cd[pageFeatures]	{"title":"Birth Control | Rush System"}
cd[parameters]	[]
sw	1920
sh	1080
v	2.9.77
r	stable
ec	2
o	30
fbp	fb.[redacted]
it	[redacted]
coo	false
es	automatic
tm	3
rqm	GET

This shows Rush has caused disclosure that the patient has engaged in a "SubscribedButtonClick," that the text of the button was "Ready to make an appointment? Schedule Appointment Now," that the user was visiting the "birth control" page of the Rush web property and the patient's Facebook Pixel identifier.

71. However, all of these transmissions are hidden from the patient. Instead, the patient only sees the following page rendered, without an indication of third-party disclosures:



72. Regardless of the next link a patient clicks to continue its communication with Rush at the Rush web-property, the source code purposefully deployed by Rush will cause transmission of their personally identifiable patient data and simultaneously re-direct the specific contents of their communication to third parties including Facebook, Google, and Bidtellect.

73. Rush uses the same tools and source code throughout its web properties, and the types of personally identifiable patient data and contents of patient communications contents Fiddler analysis determined were being transmitted to third parties without patient knowledge or authorization from the main www.rush.edu page, the Schedule Your Appointment Now link, and the birth control information page, are transmitted every time a Rush patient uses the Rush web properties, regardless of where the patient goes on the Rush websites.

The Third Parties to Whom Rush Causes Disclosures of Patient Communications and PII Include Google and Facebook

Google

74. 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 category, including the advertising services of Google DoubleClick and Google AdWords.

75. 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."[5]

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

77. Google cookies are personally identifiable. For example, Google explains the following about certain cookies that it uses:

a. "[C]ookies called 'SID' and 'HSID' contain digitally signed and encrypted records of a user's Google account ID and most recent sign-in time."[6]

b. "Most people who use Google services have a preferences cookie called 'NID' in their browsers. When you visit a Google service, the browser sends

[5] *Who Has More of Your Personal Data than Facebook? Try Google*, The Wall Street Journal (April 22, 2018) (available at https://www.wsj.com/articles/who-has-more-of-your-personal-data-than-facebook-try-google-1524398401).

[6] *Privacy & Terms, Types of Cookies Used by Google*, Google, http://web.archive.org/web/20210916060858/https:/policies.google.com/technologies/cookies?hl=en-US (archived from September 16, 2021).

this cookie with your request for a page. The NID cookie contains a unique ID Google uses to remember your preferences and other information[.]"[7]

c. "We use cookies like NID and SID to help customize ads on Google properties, like Google Search. For example, we use such cookies to remember your most recent searches, your previous interactions with an advertiser's ads or search results, and your visits to an advertiser's website. This helps us to show you customized ads on Google."[8]

d. "We also use one or more cookies for advertising we serve across the web. One of the main advertising cookies on non-Google sites is named 'IDE' and is stored in browsers under the domain doubleclick.net. Another is stored in google.com and is called ANID. We use other cookies with names such as DSID, FLC, AID, TAID, and exchange_uid. Other Google properties, like YouTube, may also use these cookies to show you more relevant ads."[9]

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

79. Google warns developers in its Personalized Advertising policies page that "Health in personalized advertising" is a "Prohibited category" for Google's personalized advertising tools. Specifically, Google's advertising policies page states:[10]

---

[7] *Privacy & Terms, Types of Cookies Used by Google*, Google, http://web.archive.org/web/20210101020222/https:/policies.google.com/technologies/cookies?hl=en-US (archived from January 1, 2021).

[8] *Id.*

[9] *Id.*

[10] *Advertising Policies Help, Personalized Advertising*, Google, http://web.archive.org/web/20191031223446/https://support.google.com/adspolicy/answer/143465?hl=en (archived from October 31, 2019).

> 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)

80. Google further states that "[a]dvertisers can't use sensitive interest categories to target ads or to promote advertisers' products or services."[11] "Health" is one such "[p]rohibited categor[y]" that Google states "can't be used by advertisers to targets ads to users or promote advertisers' products or services."

> **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

[11] *Id.*

81. Google provides instructions for web developers to anonymize IP addresses when they use Google Analytics.[12] 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."[13] 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'.[14]

82. Upon information and belief, Rush does not use Google's IP anonymization tool with Google Analytics. As a result, Rush's use of Google Analytics is not anonymous, even when no cookies are involved in the re-direction of a patient's communication.

83. Rush deploys Google tracking tools on nearly every page on its web properties, including within the patient portal, thereby causing disclosure of communications exchanged with patients to be re-directed to Google.

84. Each time a Rush patient, including Plaintiffs and Class members, visited the Rush web properties, including www.rush.edu and the MyChart patient portal, Rush caused the disclosure of communications exchanged with the patient to be re-directed to Google.

Facebook

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

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

---

[12] *Analytics Help, IP Anonymization (or IP Masking) in Universal Analytics*, Google, https://support.google.com/analytics/answer/2763052?hl=en

[13] *Id.*

[14] *Id.*

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

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

89. The Facebook Tracking Pixel is an invisible 1x1 web bug that Facebook makes available to web-developers to help developers track Facebook and other ad-driven activity on their website. Facebook warns developers that the Facebook Pixel is a personal identifier 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.

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

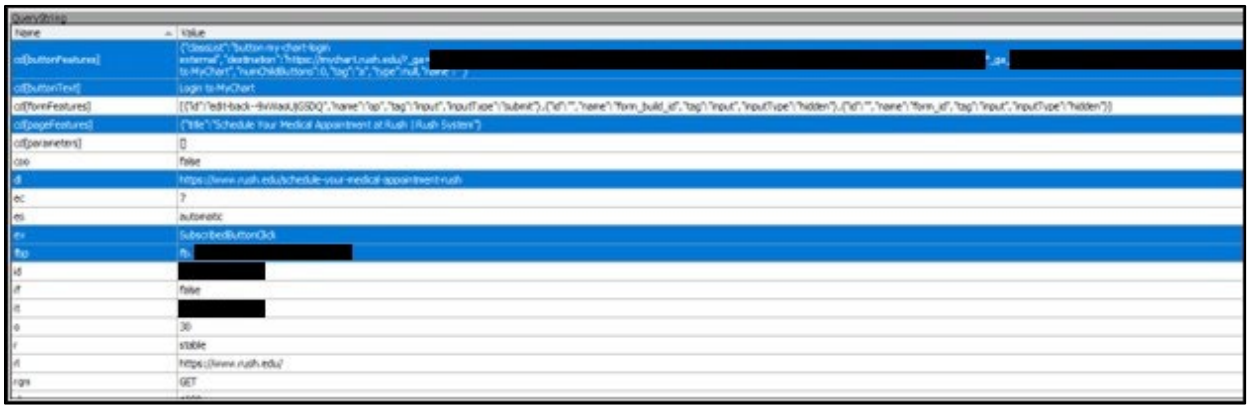
Installing The Pixel

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.

91. Rush installed the Facebook Tracking Pixel to personally identify patients who click to log-in to Rush's patient portal at www.rush.edu.

92. When a patient clicks the "MyChart" button at www.rush.edu, Rush uses the patient's personal identifiers by causing the identifiers to be transmitted to Facebook attached to the fact that the patient has exchanged a communication to log-in to the My Chart patient portal:



93. The specific identifiers that Rush uses to help Facebook acquire and record patient communications upon the My Chart Login click include the patient's IP address and cookie values, including first party cookies Rush shares with Facebook via cookie synching.

94. Each time a Rush patient, including Plaintiffs and Class members, clicked on the "MyChart" button at www.rush.edu, Rush caused the patient's personal identifiers, including the patient's IP address, to be transmitted to Facebook attached to the fact that the patient has exchanged a communication with Rush to log-in to the My Chart patient portal.

95. In addition, through the source code deployed by Rush, 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.

96. Each time a Rush patient, including Plaintiffs and Class members, clicked on the "MyChart" button at www.rush.edu, Rush caused the patient's personal identifiers, including the

c_user, datr, fr, and fbp cookies Rush uses to help Facebook identify patients, to be transmitted to Facebook attached to the fact that the patient has exchanged a communication with Rush to log-in to the My Chart patient portal.

97. 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.

98. An unskilled computer user can obtain the c_user value for any Facebook user by (1) going to the user's Facebook page, (2) right-clicking with their mouse anywhere on the background of the page, (3) selecting 'View page source,' (4) executing a control-F function for "user=" and (5) copying the number value that immediately follows "user=" in the page source code of the target Facebook user's page.

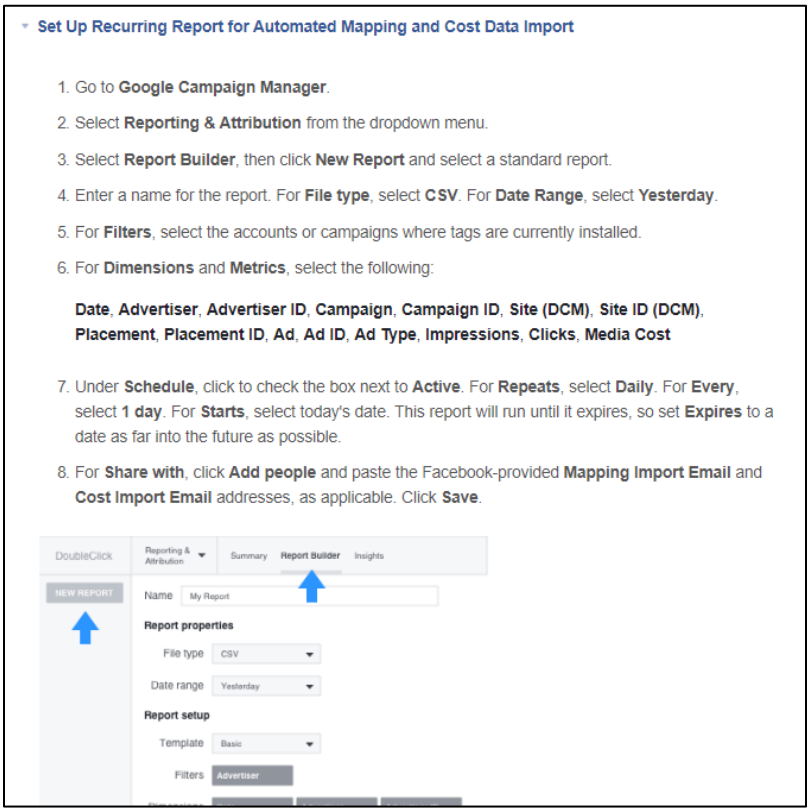
99. It is even easier to find the Facebook account associated with a c_user cookie: one simply needs to log-in to Facebook, and then type www.facebook.com/#, with # representing the c_user cookie identifier. For example, the c_user cookie value for Mark Zuckerberg is 4. Logging in to Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck.

100. The datr cookie identifies the 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.

101. The fr cookie is a Facebook identifier that is an encrypted combination of the c_user and datr cookies.[15]

102. The fbp cookie is a Facebook identifier that is set by Facebook source code and associated with Rush's use of the Facebook Tracking Pixel program. The fbp cookie emanates from Rush's web properties as a putative first-party cookie, but is transmitted to Facebook through cookie synching technology that hacks around the same-origin policy.

103. Facebook instructs developers on how to set-up their Google Campaign Manager to send automated regularly scheduled reports to Facebook:[16]



[15] *See* Gunes Acar, Brendan Van Alsenoy, Frank Piessens, Claudia Diaz, and Bart Preneel, *Facebook Tracking Through Social Plug-ins: Technical Report prepared for the Belgian Privacy Commission* (March 27, 2015) (available at https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf).

[16] *Google Campaign Manager (DoubleClick Campaign Manager)*, Meta, https://www.facebook.com/business/help/565734646951134 (last visited July 15, 2022).

104. In the absence of formal discovery and access to Rush's Google, Facebook, and Bidtellect marketing accounts, it is impossible to know whether and how much data is disclosed to Facebook through this method.

Bidtellect

105. Bidtellect is third-party company that operates a "programmatic platform" that collects and analyzes data to serve ads.[17]

106. Similar to Google Analytics and Facebook Tracking Pixel, Bidtellect provides code that is embedded into the Rush web properties for tracking and analytics to provide "cookieless" tracking and retargeting solutions.[18]

107. Bidtellect's tracking connects to "bttrack.com" to measure and record user engagement and user inputs on the Rush web property sites.[19]

108. Each time a Rush patient, including Plaintiffs and Class members, clicked on the "MyChart" button at www.rush.edu, Rush caused the patient's personally identifiable patient data to be transmitted to Bidtellect attached to the fact that the patient has exchanged a communication with Rush to log-in to the My Chart patient portal.

IP Addresses Are Personally Identifiable

109. An IP address is a number that identifies a computer connected to the Internet.

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

111. IP addresses of individual Internet users are used by websites and tracking companies to facilitate and track Internet communications.

[17] https://bidtellect.com/ last accessed September 22, 2022.
[18] *Id.*
[19] *Id.*

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

113. Under the Health Insurance Portability and Accountability Act ("HIPAA"), an IP address is considered personally identifiable information. See 45 C.F.R. § 164.514(b)(2)(i)(O).

114. Whenever a Rush patient uses the Rush web properties, Rush uses and causes the disclosure of the patient's IP addresses to third parties with each re-directed communication described herein, including patient communications about providers, conditions, treatments, appointments, bills, registration, and log-ins to the MyChart patient portal.

Internet Cookies Are Personally Identifiable

115. 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.

116. 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. Cookies can perform different functions, like saving a user's login or other site settings. Eventually, some cookies were designed to acquire and record an individual Internet user's communications and activities on websites across the Internet.

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

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

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

120. 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."

121. 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, Rush set a collection of its own cookies on patients' browsers when they visit any webpage on Rush's web properties. 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 www.rush.edu 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.

122. 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.

123. Traditionally, first- and third-party cookies were kept separate. An Internet security policy known as the same-origin policy required web browsers to prevent one web server from accessing the cookies of a separate web server. For example, although Rush can deploy source code that uses Facebook third-party cookies to help Facebook acquire and record the patient's communications, it is not permitted direct access to Facebook third-party cookie values. The reverse was also true: Facebook was not provided direct access to the values associated with first-party cookies set by Rush.

124. Data companies have designed a way to hack around the same-origin policy so that third-party data companies gain access to first-party cookies.

125. Javascript source code developed by third-party data companies and placed on a webpage by a developer such as Rush can bypass the same-origin policy to send a first-party cookie value in a tracking pixel to the third-party data company. This technique is known as "cookie synching," and it allows two cooperating websites to learn each other's cookie identification numbers for the same user. Once the cookie synching operation is completed, the two websites can exchange any information they have collected and recorded about a user that is associated with a cookie identification number. The technique can also be used to track an individual who has chosen to deploy third-party cookie blockers.

126. Whenever a Rush patient uses the Rush web properties, Rush uses and causes the disclosure of patient cookie identifiers with each re-directed communication described herein, including patient communications about providers, conditions, treatments, appointments, bills, registration, and log-ins to the MyChart patient portal.

127. Rush's cookie disclosures include the deployment of cookie synching techniques that cause the disclosure of the first-party cookie values that Rush assigns to patients to be made to third parties.

Browser-Fingerprints Are Personally Identifiable

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

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

130. 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.[20]

[20] Katarzyna Szymielewicz and Bill Dudington, *The GDPR and Browser Fingerprinting: How It Changes the Game for the Sneakiest Web Trackers*, Electronic Frontier Foundation (June 19, 2018) (available at https://www.eff.org/deeplinks/2018/06/gdpr-and-browser-fingerprinting-how-it-changes-game-sneakiest-web-trackers).

131. In 2017, researchers showed that browser fingerprinting techniques can successfully identify 99.24 percent of users.[21]

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

133. Whenever a Rush patient uses the Rush web properties,Rush uses and causes the disclosure of data sufficient to form a browser-fingerprint with each re-directed communication described herein, including patient communications about providers, conditions, treatments, appointments, bills, registration, and log-ins to the MyChart patient portal.

The Personally Identifiable Data and Communications Rush Uses and Discloses Without Patients' Knowledge, Consent, Authorization, or Further Action Has Value

134. The value of data that companies like Facebook, Google, and Bidtellect extract from people who use the Internet is well understood and generally accepted in the e-commerce industry.

135. Personal information is now viewed as a form of currency. Professor Paul M. Schwartz 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.

Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2056-57 (2004).

136. The cash value of Internet users' personal information can be quantified. In a 2015 study by the Ponemon Institute, researchers determined the value that American Internet users

[21] Yinzhi Cao, Song Li and Erik Wijmans, *(Cross-)Browser Fingerprinting via OS and Hardware Level Features*, Proceedings of the Network and Distributed Security Symposium (March 2017) (available at http://yinzhicao.org/TrackingFree/crossbrowsertracking_NDSS17.pdf).

place on their "health condition" as more valuable than any other piece of data about them, with a minimum value of $82.90.[22]

137. Medical information derived from medical providers garner even more value from the fact that it is not 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.

138. Even with restrictions on the disclosure of personally identifiable health information, a robust market exists for the trade of de-identified health data.[23]

139. Upon information and belief, Rush was compensated for its disclosures of Plaintiffs' and Class members' personally identifiable patient data and communications by the third-party recipients in the form of enhanced marketing services or other compensation.

140. Rush did not pay or offer to pay Plaintiffs or Class members for their communications or personally-identifiable patient data associated with these disclosures before or after the disclosures were made.

141. Rush profited from Plaintiffs' and Class members' information without ever intending to compensate Plaintiffs and Class members or inform them that the disclosures had been made.

---

[22] Ponemon Institute, Privacy and Security in a Connected Life: A Study of US Consumers, March 2015, available at https://vdocuments.site/privacy-and-security-in-a-connected-life-protect-personal-information-from-being.html?page=1.

[23] *See* Adam Tanner, *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/ (February 1, 2016); Sam Thielman, *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 (January 10, 2017); Adam Tanner, *The Hidden Global Trade in Patient Medical Data,* YaleGlobal Online, https://archive-yaleglobal.yale.edu/content/hidden-global-trade-patient-medical-data (last visited July 15, 2022).

142. Rush was unjustly enriched by their conduct.

Rush's Duties of Confidentiality

Duties Under Federal Law

143. Under federal law, a health care provider may not disclose personally identifiable 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).

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

145. 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).[24]

146. In its guidance for Marketing, HHS 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

[24] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule,* at 5, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (November 26, 2012).

> 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.[25]

Ancient and Modern Industry Standards of Patient Confidentiality

147. A medical provider's duty of confidentiality to patients is ancient in origin.

148. The original Hippocratic Oath, circa 400 B.C., provided that physicians must pledge, "What I may see or hear in the course of treatment or even outside of the treatment in regard to the life of man, which on no account must be spread abroad, I will keep to myself holding such things shameful to be spoken about."[26]

149. 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."[27]

150. 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.

151. AMA Code of Medical Ethics Opinion 3.2.1 provides:

> Patients need to be able to trust that physicians will protect information shared in confidence. They should feel free to fully disclose sensitive personal information to enable their physician to most effectively provide needed services. Physicians in turn have an ethical obligation to preserve the confidentiality of information gathered in association with the care of the patient.

---

[25] *Marketing*, at 1-2, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (April 3, 2003).

[26] As recited in *Brandt v. Medical Defense Associates*, 856 S.W.2d 667, 671, n. 1 (Mo. 1993)

[27] LOUIS LASAGNE, HIPPOCRATIC OATH—MODERN VERSION, *at* http://www.pbs.org/wgbh/nova/doctors/oath_modern.html.

> In general, patients are entitled to decide whether and to whom their personal health information is disclosed.[28]

152. 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.[29]

153. 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 to third parties for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity) about the purpose(s) for which access would be granted.[30]

154. 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.

---

[28] *Code of Medical Ethics Opinion 3.2.1*, AMA, https://www.ama-assn.org/delivering-care/ethics/confidentiality (last visited September 23, 2022).
[29] *Code of Medical Ethics Opinion 3.1.1*, AMA, https://www.ama-assn.org/delivering-care/ethics/privacy-health-care (last visited September 23, 2022).
[30] *Code of Medical Ethics Opinion 3.2.4*, AMA, https://www.ama-assn.org/delivering-care/ethics/access-medical-records-data-collection-companies (last visited July 15, 2022).

(emphasis added).[31]

Consumer Expectations of Patient Privacy

Confidentiality Is a Cardinal Rule of the Provider-Patient Relationship

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

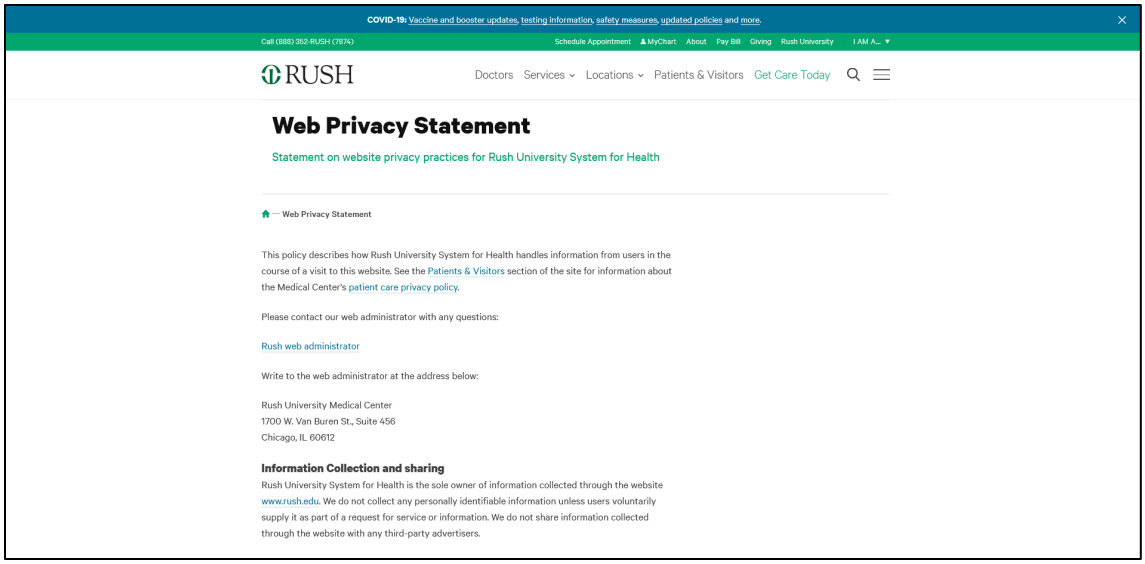
156. A recent national survey from CVS-Aetna revealed that "[p]rivacy and data security lead patients' concerns in the changing health environment." Eighty percent of survey respondents "indicated that privacy was a top concern regarding their health care, while 76 percent of individuals felt the same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

Rush Assures Patients That It Protects Their Personally Identifiable Information

157. Patients', including Plaintiffs' and Class members', reasonable expectations of privacy are further supported by express and implied promises by Rush.

158. The footer on the Rush web properties also includes a hyperlink for "Web Privacy Statement," which sends the patient to a page titled "Web Privacy Statement":

[31] *Code of Medical Ethics Opinion 3.3.2*, AMA, Conf https://www.ama-assn.org/delivering-care/ethics/confidentiality-electronic-medical-records (last visited July 15, 2022).



https://www.rush.edu/web-privacy-statement (last visited Aug. 26, 2022).

159. The "Web Privacy Statement" page does not disclose Rush's secret deployment of Facebook advertising tools on its web properties, nor the disclosure of patient PII and communications to third parties.

160. In fact, Rush's policy states the opposite. Rush says: "We do not share information collected through the website with any third-party advertisers." *Id.* It further falsely claims that "Any personally identifiable information we collect is securely stored within a database. We use standard, industry-wide procedures to protect information we receive from visitors to the website. However, as effective as encryption technology is, no security system is impenetrable." *Id.* The policy then goes on to falsely imply that it has taken steps to prevent the interception of information by third parties when, in reality, it secretly deployment interception technology—like the Facebook Pixel—to acquire patient information and the content of their communications. It states: "We cannot guarantee the security of our database, nor can we guarantee that information supplied by visitors to the website will not be intercepted while being transmitted to us over the internet." *Id.*

161. Finally, Rush also states that it "makes every effort to preserve user privacy." However, this statement is demonstrably false given that it has proactively and secretly deployment third party source code on its website.

162. A health care provider's duty of confidentiality cannot be waived via an inconspicuous, unenforceable browse-wrap privacy policy (like that used by Rush in its footer) regardless of the contents of the policy. This is especially true where the browse-wrap policy is not provided via effective notice but is only viewable if a user scrolls through multiple separate screens of content, and then is displayed on an in descript black footer on an otherwise white page.

163. In the absence of effective notice, browse-wrap statements do not create enforceable contracts against consumers.

164. The vast majority of Internet users do not read privacy policies or website terms of use. One study found that only between 0.05 to 0.22 percent of online shoppers (or 1 to 2 of every 1,000 shoppers) access online agreements—even click- or scroll-wrap agreements rather than browse-wrap agreements.[32]

165. Chief Justice John Roberts admits he does not read purported online agreements.[33]

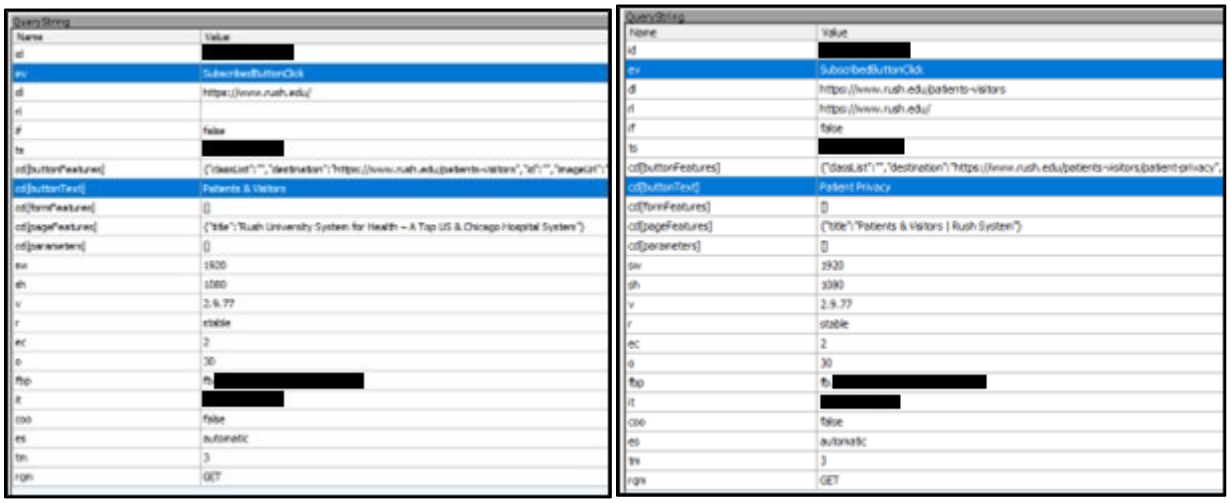
166. The cost of reading all privacy policies a consumer encounters is high. It would take an average American consumer between 181 to 304 hours per year to read the purported privacy policies of websites with which they interact.[34] This would require a consumer to devote an estimated 40 minutes per day to reading privacy policies. The time-money calculation for this

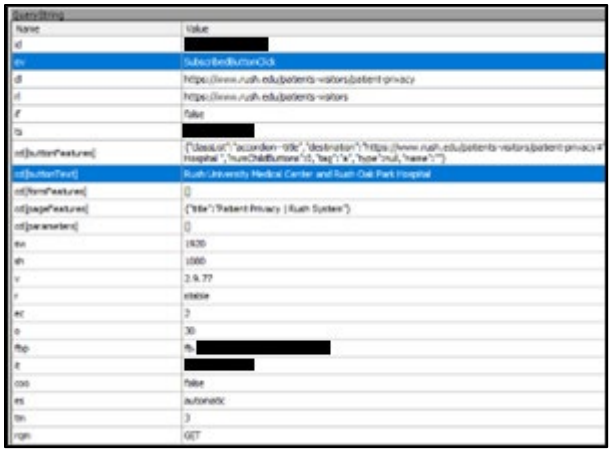
[32] Yannis Bakos, Florencia Marotta-Wurgler and David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts*, 43 J. LEGAL STUD. 1, 1 (2014).
[33] Debra Cassens Weiss, *Chief Justice Roberts Admits He Doesn't Read the Computer Fine Print*, ABA Journal (Oct. 20, 2010) ("Answering a student question, Roberts admitted he doesn't usually read the computer jargon that is a condition of accessing websites.")
[34] Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 ISJLP 543, 563 (2008).

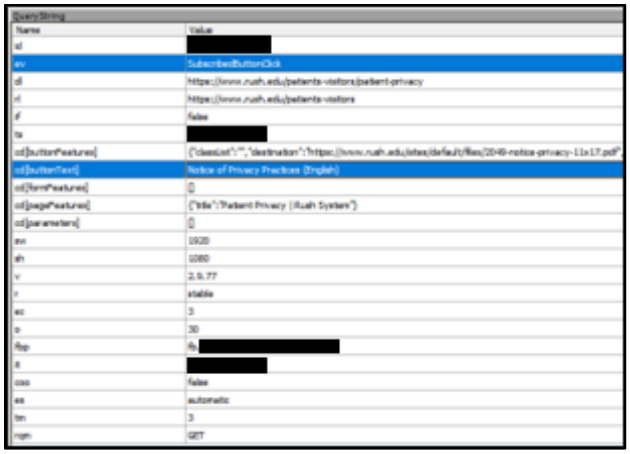
effort is between $2,553 to $5,038 per year per consumer for a collective national cost of $559.7 billion to $1.1 trillion per year.

167. Regardless, it is reasonable for a patient to assume that their health care providers' privacy policies are consistent with their providers' duties of confidentiality and patient expectations of privacy.

168. To comply with the requirement of posting the HIPAA notice on its web-property. To find the policy, patients must navigate from the homepage to the "Patients & Visitors" tab, click on the "Patient Privacy" button, then click on the correct facility (*e.g.* Rush University Medical Center or Rush Oak Park Hospital), and then click on the "Notice of Privacy Practices" link. However, unbeknownst to the patient, these *patient privacy-related steps* were all being contemporaneously transmitted to Facebook:







169. The very term "Privacy Policy," in general, and as used by Rush, is deceptive. Research has consistently shown that a majority of Americans who see that a website has a "Privacy Policy" falsely believe that the company with the policy cannot disclose information about them without their consent.

170. By taking such action of linking the privacy link to the HIPAA Notice of Privacy Practices, Rush gives patients the impression that it treats their communications at its web property with the same confidentiality that it treats patient communications at its physical properties.

171. As a matter of law, there is no exception in HIPAA for communications between patients and providers that occur over the Internet.

172. Rush's Notice of Privacy Practices promises the following:

a. "We are required by applicable federal and state law to maintain the privacy of your medical information."

b. "[W]e will not sell your medical information or use or disclose your medical information for marketing without your prior written authorization."

c. "Unless you give us a written authorization, we cannot use or disclose your medical information for any reason except those described in this notice."

d. "We will not use or disclose your protected health information for marketing purposes without your written authorization. Marketing is defined as receipt of payment from a third party for communicating with you about a product or service marketed by the third party."

https://www.rush.edu/sites/default/files/2049-notice-privacy-11x17.pdf (last visited Aug. 26, 2022).

173. While it is true that Rush is "required by applicable federal and state law to maintain the privacy of your medical information, " Rush's claims that it will not disclose patient medical information without authorization is false and misleading given that it routinely, automatically, secretly, and without authorization, discloses patient medical information to third parties including Facebook, Google and Bidtellect.

CLASS ACTION ALLEGATIONS

174. Plaintiff re-alleges and incorporates by reference the allegations set forth above.

175. Plaintiffs bring this action as a class action pursuant to Rules 23(a), 23(b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of two classes, defined as follows:

Patient Class

During the fullest period allowed by law, all persons who are, or were, patients of Rush or any of its affiliates and accessed Rush's MyChart patient portal that causes transmission of personally identifiable data and communications to be made to third-parties.

Illinois Class

During the fullest period allowed by law, all residents of Illinois who are, or were, patients of Rush or any of its affiliates and accessed Rush's MyChart patient portal that causes transmission of personally identifiable data and communications to be made to third-parties.

176. Excluded from the Patient Class and the Illinois Class (collectively the "Class") are Rush and any of its members, affiliates, parents, subsidiaries, officers, directors, employees,

successors, or assigns; and the Court staff assigned to this case and their immediate family members. Plaintiffs reserve the right to modify or amend the Class definition, as appropriate, during the course of this litigation.

177. This action has been brought and may properly be maintained on behalf of the Class proposed herein under the criteria of Rule 23 of the Federal Rules of Civil Procedure.

178. **Numerosity—Federal Rule of Civil Procedure 23(a)(1)** – Class members are so numerous that their individual joinder is impracticable. The precise number of Class members and their identities are unknown to Plaintiffs at this time but will be determined through discovery through the records of the Defendant.

179. **Commonality and Predominance—Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3)** – Common questions of law and fact exist and predominate over questions affecting only individual Class members. These common legal and factual questions include the following:

a. Whether Defendant's practices relating to disclosures of Plaintiffs' and patient Class Members' personally identifiable data and communications to third parties were intentional;

b. Whether Defendant profited from disclosures to the third parties;

c. Whether Defendant's conduct violated the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq*.;

d. Whether Defendant's practices alleged herein were unfair, deceptive, and/or unlawful in any respect, thereby violating the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq*.;

e. Whether Defendant's practices alleged herein were unfair trade practices, thereby violating the Illinois Deceptive Trade Practices Act, 815 ILCS 510/1 *et seq*.;

f. Whether Defendant's practices constitute an unauthorized intrusion upon seclusion;

g. Whether Defendant's practices constitute breach of implied duty of confidentiality;

h. Whether Defendant's conduct harmed and continues to harm Plaintiffs and Class members, and if so, the extent of the injury;

i. Whether and to what extent Plaintiffs and Class members are entitled to damages and other monetary relief;

j. Whether and to what extent Plaintiffs and Class members are entitled to equitable relief, including, but not limited to, a preliminary and/or permanent injunction; and

k. Whether and to what extent Plaintiffs and Class members are entitled to attorney fees and costs.

180. **Typicality—Federal Rule of Civil Procedure 23(a)(3)** – Plaintiffs' claims are typical of the claims of the Patient Class and the Illinois Class and Plaintiffs have substantially the same interest in this matter as other Class members. Plaintiffs have no interests that are antagonistic to, or in conflict with, the interests of the other members of the Class. Plaintiffs' claims arise out of the same set of facts and conduct as all other Class members. Plaintiffs and all Class members are patients of Rush who used the Defendant's web-property set-up by Rush for patients, and are

victims of Rush's unauthorized disclosures to third-parties. All claims of the Plaintiffs and Class members are based on Rush's wrongful conduct and unauthorized disclosures.

181. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4)** – Plaintiffs will fairly and adequately protect the interests of Class Members. Plaintiffs have retained competent counsel experienced in complex class action privacy litigation and Plaintiffs will prosecute this action vigorously. Plaintiffs have no interests adverse or antagonistic to those of the Class.

182. **Declaratory and Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2)** – Rush acted or refused to act on grounds generally applicable to Plaintiffs and the other Class members, thereby making appropriate final injunctive relief and/or declaratory relief, as described below.

183. **Superiority—Federal Rule of Civil Procedure 23(b)(3)** – A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are small compared with the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for the Class Members, on an individual basis, to obtain effective redress for the wrongs done them. Furthermore, even if Class Members could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and

comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

184. Additionally, the Class may be certified under Rule 23(b)(1) or (b)(2) because:

a. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for Defendant;

b. The prosecution of separate actions by individual Class Members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and/or

c. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final and injunctive relief with respect to the Class Members as a whole.

COUNT I
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2510 *et seq.*
On Behalf of Plaintiffs and the Patient Class

185. Plaintiffs individually and on behalf of the other Patient Class members, repeat and reallege Paragraphs 1 through 184, as if fully alleged herein.

186. The ECPA protects both the sending and receipt of communications.

187. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral, or electronic communication is intercepted.

188. A violation of the ECPA occurs where any person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any . . . electronic communication" or "intentionally discloses, or endeavors to disclose, to any other person the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication" or "intentionally uses, or endeavors to use, the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication." 18 U.S.C. §§ 2511(1)(a), (c)-(d).

189. In addition, "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication [ ] while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

190. "Intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

191. "Electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

192. "Contents" includes "any information relating to the substance, purport, or meaning" of the communication at issue. 18 U.S.C. § 2510(8).

193. An "electronic communication service" means "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

194. Plaintiffs and Patient Class members' interactions with Rush's web properties, including the MyChart patient portal, and their online communications with Rush are electronic communications under the ECPA.

195. Rush's MyChart patient portal is an electronic communication service under the ECPA.

196. Whenever Plaintiffs and Patient Class members interacted with Rush's web properties, including Rush's MyChart patient portal, Rush, through the source code it imbedded and ran on its web properties, contemporaneously and intentionally intercepted, and endeavored to intercept Plaintiffs' and Patient Class members' electronic communications without authorization or consent.

197. Whenever Plaintiffs and Patient Class members interacted with Rush's web properties, including Rush's MyChart patient portal, Rush, through the source code it imbedded and ran on its web properties, contemporaneously and intentionally disclosed, and endeavored to disclose the contents of Plaintiffs' and Patient Class members' electronic communications to third parties, including Facebook, Google, and Bidtellect, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA.

198. Whenever Plaintiffs and Patient Class members interacted with Rush's web properties, including Rush's MyChart patient portal, Rush, through the source code it imbedded and ran on its web properties, contemporaneously and intentionally used, and endeavored to use the contents of Plaintiffs' and Patient Class members' electronic communications, for purposes

other than providing health care services to Plaintiffs and Patient Class members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA.

199. Whenever Plaintiffs and Patient Class members interacted with Rush's web properties, including Rush's MyChart patient portal, Rush, through the source code it imbedded and ran on its web properties, contemporaneously and intentionally redirected the contents of Plaintiffs' and Class members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook, Google, and Bidtellect.

200. Whenever Plaintiffs and Patient Class members interacted with Rush's web properties, including Rush's MyChart patient portal, Rush, through the source code it imbedded and ran on its web properties, contemporaneously and intentionally divulged the contents of Plaintiffs' and Class members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook, Google, and Bidtellect.

201. Rush intentionally intercepted and used the contents of Plaintiffs' and Patient Class members' electronic communications for the unauthorized purpose of disclosing and, on information and belief, profiting from, Plaintiffs' and Patient Class members' communications by selling the contents to third parties including Facebook, Google, and Bidtellect.

202. Plaintiffs and Patient Class members did not authorize Rush to acquire the content of their communications for purposes of sharing and selling the personal information contained therein.

203. As a direct and proximate result of Rush's violation of the ECPA, Plaintiffs and Patient Class members were damaged by Rush's conduct in that:

a. Rush harmed Plaintiffs' and Patient Class members' interest in privacy;

b. Sensitive and confidential information that Plaintiff and Patient Class members intended to remain private is no more;

c. Rush eroded the essential confidential nature of the provider-patient relationship;

d. Rush took something of value from Plaintiffs and Patient Class members and derived benefit therefrom without Plaintiffs' and Patient Class members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;

e. Plaintiffs and Patient Class members did not get the full value of the medical services for which they paid, which included Rush's duty to maintain confidentiality; and

f. Rush's actions diminished the value of Plaintiffs and Patient Class members' personal information.

204. Plaintiffs, individually, on behalf of the Patient Class members, seek all monetary and non-monetary relief allowed by law, including actual damages, statutory damages, punitive damages, preliminary and other equitable or declaratory relief, and attorneys' fees and costs.

COUNT II
BREACH OF THE IMPLIED DUTY OF CONFIDENTIALITY
On Behalf of Plaintiffs and the Patient Class

205. Plaintiffs individually and on behalf of the other Patient Class members, repeat and reallege Paragraphs 1 through 184, as if fully alleged herein.

206. Plaintiffs and Patient Class members were patients of Rush and received health care services from Rush.

207. As part of establishing and continuing the health care services provider/patient relationship between Rush and Plaintiffs and Patient Class members, Rush agreed to keep Plaintiffs' and Patient Class members information confidential.

208. There is a duty of confidentiality implied in every health care provider and patient relationship, akin to an implied contract, such that health care services providers may not disclose confidential information acquired through the health care provider-patient relationship. *See, e.g.*, *Geisberger v. Willuhn*, 72 Ill. App. 3d 435, 438 (1979).

209. The implied duty of confidentiality is at least as extensive as Rush's statutory obligations as a health care services provider to maintain patient confidentiality.

210. Under the Illinois' Medical Patient Rights Act ("MPRA") "health care provider[s]" must "refrain from disclosing the nature or details of services provided to patients." 410 ILCS § 50/3.

211. Under 735 ILCS 5/8-802, "[n]o physician or surgeon shall be permitted to disclose any information he or she may have acquired in attending any patient in a professional character."

212. Rush is obligated to protect the confidentiality of patient information under HIPPA.

213. Rush also may not disclose personally identifiable 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).

214. Rush's web property, www.rush.edu, links to a HIPAA notice that acknowledges Rush's duty of confidentiality, including assuring Plaintiffs and Patient Class members that Rush

will protect the confidentiality of their data and communications. The notice further assures Plaintiffs and Patient Class members that Rush will not use their data and communications for marketing purposes without express written authorization.

215. Plaintiffs and Patient Class members performed all required conditions of their implied contracts with Rush.

216. Rush breached the implied duty of confidentiality to Plaintiffs and Patient Class members by intentionally deploying source code at its web property that caused the transmission of personally identifiable patient data and communications to third parties including Facebook, Google, and Bidtellect.

217. As a direct and proximate result of Rush's breach of the implied duty of confidentiality, Plaintiffs and Patient Class members were damaged in that:

a. Rush harmed Plaintiffs' and Patient Class members' interest in privacy;

b. Sensitive and confidential information that Plaintiffs and Patient Class members intended to remain private is no more;

c. Rush eroded the essential confidential nature of the provider-patient relationship;

d. Rush took something of value from Plaintiffs and Patient Class members and derived benefit therefrom without Plaintiffs' and Patient Class members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;

e. Plaintiffs and Patient Class members did not get the full value of the medical services for which they paid, which included Rush's duty to maintain the confidentiality of their patient information; and

f. Rush's actions diminished the value of Plaintiffs' and Patient Class members' personal information.

218. Plaintiffs seek all monetary and non-monetary relief allowed by law.

COUNT III
VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815 ILCS 505/1, *et seq*.
On Behalf of Plaintiffs and the Illinois Class

219. Plaintiffs individually and on behalf of the other Illinois Class members, repeat and reallege Paragraphs 1 through 184, as if fully alleged herein.

220. Rush is a "person" as defined by ILCS § 505/1(c).

221. Plaintiffs and the other Illinois Class members are "consumers" as defined by 815 ILCS § 505/1(e).

222. Rush's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 ILCS. § 505/1(f).

223. Rush's unfair acts and practices against Plaintiffs and the other Illinois Class members occurred in the course of trade or commerce in Illinois, arose out of transactions that occurred in Illinois, and/or harmed individuals in Illinois.

224. Plaintiffs and Illinois Class members received and paid for health care services from Rush.

225. Plaintiffs and Illinois Class members used Rush's web properties, including the MyChart patient portal, in connection with receiving health care services from Rush.

226. Plaintiffs' and Illinois Class members' payments to Rush for health care services were for household and personal purposes.

227. Rush's practice of disclosing Plaintiffs' and Illinois Class members' personally identifiable data and re-directing their communications to third parties without authorization,

consent, or knowledge is a deceptive, unfair, and unlawful trade act or practice, in violation of 815 ILCS § 505/2.

228. Rush's unfair business practices were targeted at all Rush patients, including Plaintiffs and the other Illinois Class members.

229. Rush's representations and omissions were material because they were likely to deceive reasonable consumers about the privacy, security, and use of their personally identifiable patient data and communications when using the Rush web property, including the MyChart patient portal.

230. Rush intended to mislead Plaintiffs and the other Illinois Class members and induce them to rely on its misrepresentations and omissions.

231. Rush's surreptitious collection and disclosure of Plaintiffs' and the Illinois Class members' personally identifiable data and communications to third parties involves important consumer protection concerns.

232. The relief requested by Plaintiffs and the other Illinois Class members, would provide redress for the harms Rush caused not just to Plaintiffs, but to all other Illinois Class members.

233. Plaintiffs and the Illinois Class members were injured and have suffered damages as a direct and proximate result of Rush's unfair acts and practices.

234. Plaintiffs' and the Illinois Class members' injuries were proximately caused by Rush's unfair and deceptive business practices.

235. As a result of Rush's conduct, Rush has been unjustly enriched.

236. Rush's acts caused substantial injury that Plaintiffs and the Illinois Class members could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

237. Rush acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud and Deceptive Business Practices Act, and recklessly disregarded Plaintiffs' and the Illinois Class members' rights.

238. As a direct and proximate result of Rush's unfair, unlawful, and deceptive acts and practices, Plaintiffs and the Illinois Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including overpaying for Rush's health care services; and loss of value of their personally identifiable patient data and communications.

239. As a direct and proximate result of Rush's unfair, unlawful, and deceptive acts and practices, Plaintiffs and the Illinois Class members were also damaged by Rush's conduct in that:

a. Rush harmed Plaintiffs' and Illinois Class members' interest in privacy;

b. Sensitive and confidential information that Plaintiff and Illinois Class members intended to remain private is no more;

c. Rush eroded the essential confidential nature of the provider-patient relationship;

d. Rush took something of value from Plaintiffs and Illinois Class members and derived benefit therefrom without Plaintiffs' and Illinois Class members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;

e. Plaintiffs and Illinois Class members did not get the full value of the medical services for which they paid, which included Rush's duty to maintain confidentiality; and

f. Rush's actions diminished the value of Plaintiffs and Illinois Class members' personal information.

240. Plaintiffs, individually, on behalf of the Illinois Class members, seek all monetary and non-monetary relief allowed by law.

COUNT IV
VIOLATION OF THE ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT
815 ILCS §§ 510/2, *et seq*.
On Behalf of Plaintiffs and the Illinois Class

241. Plaintiffs individually and on behalf of the other Illinois Class members, repeat and reallege Paragraphs 1 through 184, as if fully alleged herein.

242. Rush is a "person" as defined by 815 ILCS § 510/1(5).

243. Rush engaged in deceptive trade practices in the conduct of its business, in violation of 815 ILCS § 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

244. Rush's practice of disclosing Plaintiffs' and Illinois Class members' personally identifiable data and re-directing their communications to third parties without authorization, consent, or knowledge is a deceptive trade practice, in violation of 815 ILCS § 510/2(a).

245. Rush's practice of disclosing Plaintiffs' and Illinois Class members' personally identifiable data and re-directing their communications to third parties without authorization, consent, or knowledge was willful.

246. Rush's practice of disclosing Plaintiffs' and Illinois Class members' personally identifiable data and re-directing their communications to third parties without authorization, consent, or knowledge was intentional.

247. Rush's representations and omissions were material because they were likely to deceive reasonable consumers about the privacy, security, and use of their personally identifiable patient data and communications when using the Rush web property, including the MyChart patient portal.

248. The above unfair and deceptive practices and acts by Rush were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and the Illinois Class members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

249. As a direct and proximate result of Rush's unfair, unlawful, and deceptive trade practices, Plaintiffs and the Illinois Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including overpaying for Rush's health care services; and loss of value of their personally identifiable patient data and communications.

250. As a direct and proximate result of Rush's unfair, unlawful, and deceptive acts and practices, Plaintiffs and the Illinois Class members were also damaged by Rush's conduct in that:

a. Rush harmed Plaintiffs' and Illinois Class members' interest in privacy;

b. Sensitive and confidential information that Plaintiff and Illinois Class members intended to remain private is no more;

c. Rush eroded the essential confidential nature of the provider-patient relationship;

d. Rush took something of value from Plaintiffs and Illinois Class members and derived benefit therefrom without Plaintiffs' and Illinois Class members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;

e. Plaintiffs and Illinois Class members did not get the full value of the medical services for which they paid, which included Rush's duty to maintain confidentiality; and

f. Rush's actions diminished the value of Plaintiffs and Illinois Class members' personal information.

251. Plaintiffs and the Illinois Class members are patients of Rush and need access to Rush's web properties, including www.rush.edu and the MyChart portal, in connection with receiving health care from Rush. Because Plaintiffs and Class members need to, and so will continue to use Rush's web properties in the future, if Rush's unfair, unlawful, and deceptive trade practices are allowed to continue, Plaintiffs and Illinois Class members are likely to suffer continuing harm in the future.

252. Plaintiffs and the Illinois Class members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

COUNT V
INVASION OF PRIVACY – INTRUSION UPON SECLUSION
On Behalf of Plaintiffs and the Illinois Class

253. Plaintiffs individually and on behalf of the other Illinois Class members, repeat and reallege Paragraphs 1 through 184, as if fully alleged herein.

254. Plaintiffs' and Illinois Class members' communications with Rush constitute private conversations, matters, and data.

255. Plaintiffs and Illinois Class Members have a reasonable expectation that Rush would not disclose personally identifiable patient data and communications to third parties for marketing purposes without Plaintiffs and other Illinois Class members authorization, consent, knowledge, or any further action on the patient's part.

256. Rush, a health care provider, has a duty to keep personally identifiable patient data and communications confidential.

257. Rush expressly promised to maintain the confidentiality of personally identifiable patient data and communications in its HIPAA Notice of Privacy Practices and Web and Internet Policies.

258. Rush intruded upon Plaintiffs' and Illinois Class members' seclusion by deploying source code that caused the transmission of Plaintiffs' and Illinois Class members' personally identifiable data and the contents of communications Plaintiffs and Illinois Class members exchanged with their health care providers to third parties including Facebook, Google, and Bidtellect.

259. Plaintiffs and Illinois Class members did not authorize, consent, know about, or take any action to indicate consent to Rush's conduct alleged herein.

260. Plaintiffs' and Illinois Class members' personally identifiable data and communications are the type of sensitive, personal information that one normally expects will be protected from disclosure to unauthorized parties by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiffs' and Illinois Class members' personally identifiable data and communications, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

261. Rush's conduct described herein was intentional.

262. Rush's conduct in disclosing Plaintiffs' and Illinois Class members' personally identifiable data and communications to third parties was and is highly offensive to a reasonable person.

263. Rush's willful and reckless conduct in allowing access to and disclosure of Plaintiffs' and Illinois Class members' sensitive, personally identifiable data and communications to unauthorized third parties is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

264. As a direct and proximate result of Rush's intrusion upon their seclusion, Plaintiffs and Illinois Class members were damaged by Rush's intrusion in that:

g. Rush harmed Plaintiffs' and Illinois Class members' interest in privacy;

h. Sensitive and confidential information that Plaintiff and Illinois Class members intended to remain private is no more;

i. Rush eroded the essential confidential nature of the provider-patient relationship;

j. Rush took something of value from Plaintiffs and Illinois Class members and derived benefit therefrom without Plaintiffs' and Illinois Class members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;

k. Plaintiffs and Illinois Class members did not get the full value of the medical services for which they paid, which included Rush's duty to maintain confidentiality; and

l. Rush's actions diminished the value of Plaintiffs and Illinois Class members' personal information.

265. As a result of the invasion of privacy caused by Rush, Plaintiffs and Illinois Class members suffered and will continue to suffer damages and injury as set forth herein.

266. Plaintiffs and Illinois Class members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other Class members, respectfully requests relief against Rush as set forth below:

a. Entry of an order certifying the proposed Patient Class and Illinois Class pursuant to Federal Rule of Civil Procedure 23;

b. Entry of an order appointing Plaintiffs as representatives of the Patient Class and Illinois Class;

c. Entry of an order appointing Plaintiffs' counsel as Class Counsel for the Patient Class and the Illinois Class;

d. Entry of an order for injunctive and declaratory relief as described herein, including but not limited to:

i. Enjoining Rush, its affiliates, associates, officers, employees and agents from transmitting or disclosing Plaintiffs' and Class members' personally identifiable patient data and the contents of their communications to unauthorized third parties;

ii. Enjoining Rush, its affiliates, associates, officers, employees and agents from taking Plaintiffs' and Class members' personally identifiable patient data and the contents of their communications, and any other data except that for which appropriate notice and consent is provided;

iii. Mandating that Rush, its affiliates, associates, officers, employees and agents hire third-party monitors for a period of at least three years to ensure that all the above steps have been taken; and

iv. Mandating that Rush, its affiliates, associates, officers, employees and agents provide written verifications on a quarterly basis to the court and counsel for the Plaintiffs in the form of a declaration under oath that the above steps have been satisfied.

e. Enter judgment in favor of Plaintiffs and each of the other Class members for damages suffered as a result of Rush's conduct alleged herein, including compensatory, statutory, and punitive damages; as well as equitable relief including restitution and disgorgement, to include interest and prejudgment interest;

f. Award Plaintiffs their reasonable attorneys' fees and costs; and

g. Grant such other and further legal and equitable relief as the court deems just and equitable.

JURY DEMAND

Plaintiffs demand a trial by jury on all claims so triable.

Dated: September 30, 2022

Respectfully Submitted,

/s/ Amy E. Keller
DICELLO LEVITT LLC
Adam J. Levitt
Amy E. Keller
Nada Djordjevic
Sharon Cruz
Ten North Dearborn St., Sixth Floor
Chicago, Illinois 60602
Tel.: (312) 214-7900
Fax.: (312) 253-1443
alevitt@dicellolevitt.com
akeller@dicellolevitt.com
ndjordjevic@dicellolevitt.com
scruz@dicellolevitt.com

DICELLO LEVITT LLC
David A. Straite*
Corban Rhodes*
485 Lexington Ave., 10th Floor
New York, NY 10017
Tel.: (646) 933-1000
Fax.: (646) 494-9648
dstraite@dicellolevitt.com
crhodes@dicellolevitt.com

SIMMONS HANLY CONROY LLC
Jason 'Jay' Barnes*
112 Madison Ave., 7th Floor
New York, NY 10016
Tel.: (212) 784-6400
Fax: (212) 213-5949

jaybarnes@simmonsfirm.com

Pro hac vice applications forthcoming

ClassAction.org
