

IN THE COURT OF COMMON PLEAS OF ALLEGHENY COUNTY, PENNSYLVANIA

**JANE DOE I and JANE DOE
II, on behalf of themselves and
all others similarly situated,**

Plaintiffs,

v.

**UPMC, a Pennsylvania
Nonprofit, Non-Stock
Corporation,**

Defendant.

CIVIL ACTION

Case No. _____

CODE ____ CLASS ACTION

COMPLAINT (REDACTED)

FILED ON BEHALF OF PLAINTIFFS, JANE
DOE I and JANE DOE II

Counsel of Record:

James C. Shah (ID No. 80337)
Nathan Zipperian (ID No. 202585)
Michael Ols (ID No. 326144)
SHEPHERD, FINKELMAN, MILLER &
SHAH, LLP
1845 Walnut Street, Suite 806
Philadelphia, PA 19103
Telephone: (610) 891-9880
Facsimile: (866) 300-7367
jshah@sfmslaw.com
nzipperian@sfmslaw.com
mols@sfmslaw.com

Jay Barnes
Mitchell Breit
SIMMONS HANLY CONROY
112 Madison Avenue
New York, New York 10016-7416
Telephone: 212-784-6400
Fax: 212-213-5949
jaybarnes@simmonsfirm.com
mbreit@simmonsfirm.com

JURY TRIAL DEMANDED

IN THE COURT OF COMMON PLEAS OF ALLEGHENY COUNTY, PENNSYLVANIA

**JANE DOE I and JANE DOE II, on
behalf of themselves and all others
similarly situated,**

Plaintiffs,

v.

**UPMC, a Pennsylvania Nonprofit, Non-
Stock Corporation,**

Defendant.

CIVIL ACTION

Case No. _____

CLASS ACTION

NOTICE TO DEFEND

You have been sued in court. If you wish to defend against the claims set forth in the following pages, you must take action within twenty (20) days after this complaint and notice are served, by entering a written appearance personally or by attorney and filing in writing with the court your defenses or objections to the claims set forth against you. You are warned that if you fail to do so the case may proceed without you and a judgment may be entered against you by the court without further notice for any money claimed in the complaint or for any other claim or relief requested by the plaintiff. You may lose money or property or other rights important to you.

YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER AT ONCE. IF YOU DO NOT HAVE A LAWYER, GO TO OR TELEPHONE THE OFFICE SET FORTH BELOW. THIS OFFICE CAN PROVIDE YOU WITH INFORMATION ABOUT HIRING A LAWYER. IF YOU CANNOT AFFORD TO HIRE A LAWYER, THIS OFFICE MAY BE ABLE TO PROVIDE YOU WITH INFORMATION ABOUT AGENCIES THAT MAY OFFER LEGAL SERVICES TO ELIGIBLE PERSONS AT A REDUCED FEE OR NO FEE.

LAWYER REFERRAL SERVICE
The Allegheny County Bar Association
11th Floor Koppers Bldg.
436 Seventh Avenue, Pittsburgh, PA 15219
TELEPHONE: 412-261-5555

IN THE COURT OF COMMON PLEAS OF ALLEGHENY COUNTY, PENNSYLVANIA

**JANE DOE I and JANE DOE II, on
behalf of themselves and all others
similarly situated,**

Plaintiffs,

v.

**UPMC, a Pennsylvania Nonprofit,
Non-Stock Corporation,**

Defendant.

CIVIL ACTION

Case No. _____

CLASS ACTION

CLASS ACTION COMPLAINT

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

NATURE OF THE ACTION

1. Plaintiffs are patients of Defendant, UPMC (hereafter “UPMC” or “Defendant”).
2. As patients, Plaintiffs have reasonable expectations of privacy that UPMC, their health care provider, will not disclose their personal information or the content of their

communications exchanged with UPMC to third parties for marketing purposes without patient knowledge, consent, or authorization.

3. In Pennsylvania, medical providers have an obligation to their patients to keep communications, diagnoses, and treatment completely confidential.

4. Patients are aware of the promises of discretion contained within the Hippocratic Oath and must be able to rely on those promises and obligations.

5. UPMC maintains web properties, including at www.UPMC.com and an online patient portal at the subdomain, MyUPMC.upmc.com, through which it encourages patients to exchange communications to search for a doctor, learn more about their conditions and treatments, access medical records and test results, and make appointments.

6. UPMC expressly and impliedly promises Plaintiffs and other of its patients that UPMC will maintain the privacy and confidentiality of communications that patients exchange with UPMC at the web-property, UPMC.com, and the patient portal myupmc.upmc.com.

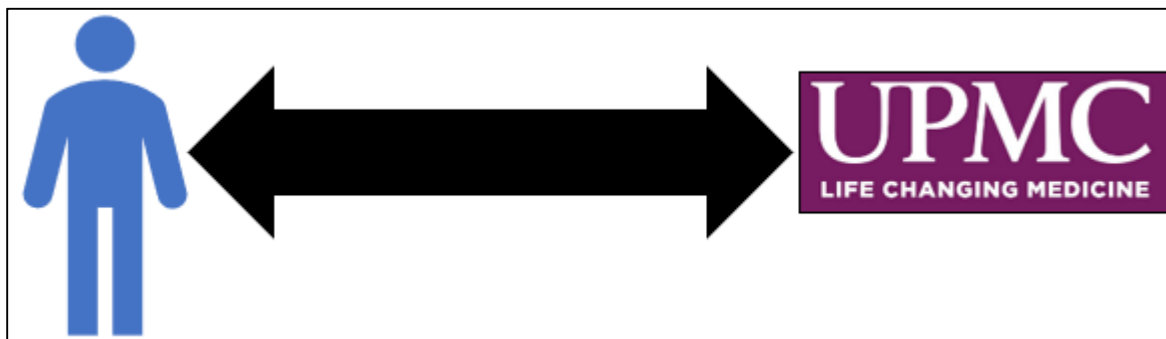
7. For example, UPMC promises:

- a. For all marketing activities other than face-to-face discussions or inexpensive promotional gifts, UPMC “will obtain [patient] written permission before using or sharing [patient] health information” with any third party;
- b. UPMC “will not sell your identifiable health information to others without authorization;”
- c. UPMC “keep[s] the personal information of [its] patients and members in the strictest confidence;” and
- d. “We do not disclose identifiable personal information to other organizations.”

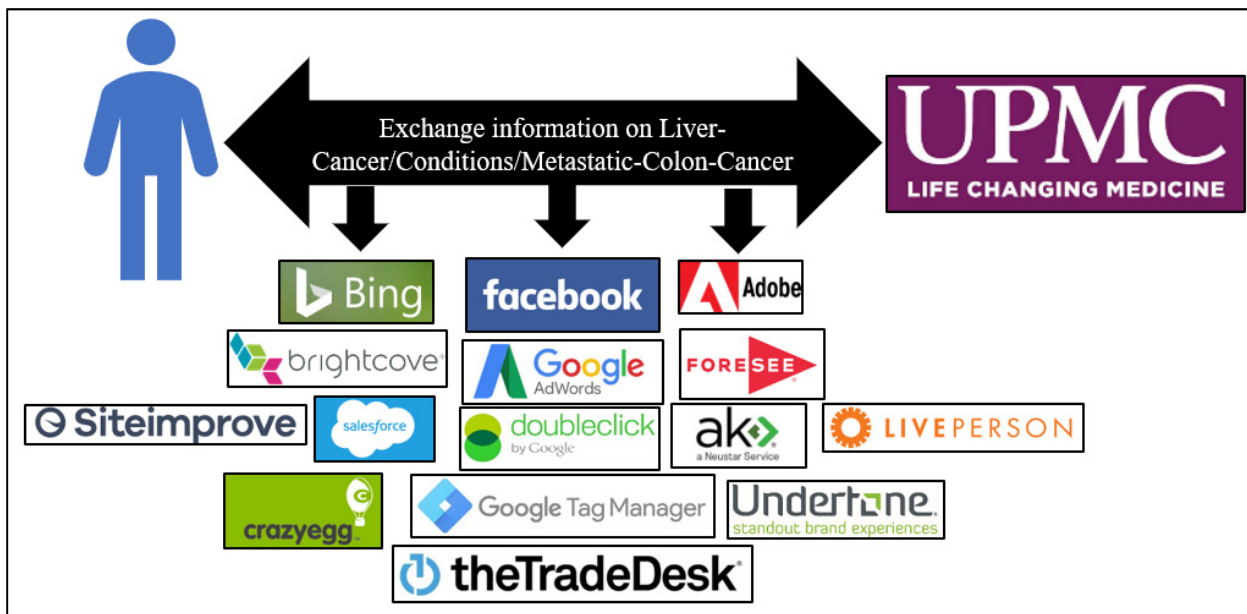
8. Based on patients’ reasonable expectations of privacy, UPMC’s express and

implied promises, and statutes, rules, and industry standards protecting patients' health and communications privacy, patients expect that the communications they exchange with UPMC at UPMC.com and myupmc.upmc.com are between the patient and UPMC only and not shared with third parties.

9. A patient's reasonable expectation for the communications with UPMC is illustrated as follows:



10. Instead, when a patient exchanges a communication with UPMC at its web-property, UPMC re-directs the patient's personal information and the contents of their communication to numerous third parties, illustrated as follows:



11. UPMC does not disclose and patients do not authorize the re-direction of patient personal information and the content of patient communications to any of these third parties.

12. These and substantially similar re-directions occur even after a patient has formally signed-in to the patient portal at myupmc.upmc.com and continue while a patient is logged in to the “secure” website as a patient.

13. UPMC causes the unauthorized transmissions of patient data and communications through computer source code that it deploys to command patient computing devices to transmit the data to third parties through invisible web-bugs that include, but are not limited to, Facebook, Google, Twitter, Adobe, Microsoft, Oracle, Trade Desk, Neustar, Everest Technologies, Site Improve, Krux Digital, Undertone, and Acxiom.

14. UPMC’s conduct violates common law and privacy laws of the Commonwealth of Pennsylvania, including: (1) breach of provider-patient confidentiality; (2) violation of § 5703 of the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa.C.S.A. § 5701, *et seq.*; (3) violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§201-1, *et seq.*; (4) identity theft, in violation of 42 Pa.C.S.A. § 4120, as made actionable through 42 Pa.C.S. § 8315; and (5) negligence.

PARTIES TO THE ACTION

15. Jane Doe I is a patient of UPMC residing in Pennsylvania. Jane Doe I exchanged private communications with UPMC at its web-property, UPMC.com, and the subdomain containing the patient portal at myupmc.upmc.com.

16. Jane Doe II is a patient of UPMC residing in Pennsylvania. Jane Doe II exchanged private communications with UPMC at its web-property, UPMC.com, and the subdomain containing the patient portal at myupmc.upmc.com.

17. UPMC is a Pennsylvania non-profit and non-stock corporation with its principal place of business in Pittsburgh, Pennsylvania. UPMC is a covered entity under 42 U.S.C. § 1320d and 45 C.F.R. 160-164 (the Health Insurance Portability and Accountability Act or “HIPAA”). Defendant owns and operates multiple health care properties throughout Pennsylvania, including the web-properties it operates out of Pittsburgh.

JURISDICTION AND VENUE

18. This Court has jurisdiction pursuant to 42 Pa.C.S. § 931 in that the matters complained of herein occurred within the County of Allegheny and this Court has original jurisdiction over all cases not exclusively assigned to another court.

19. Venue is proper before this Court pursuant to 42 Pa.C.S. § 931(c) and Pa. R. Civ. P. 1006(b) and 2179(a). Venue is proper as to Defendant because Defendant carries on regular business in Allegheny County and because each cause of action herein arose in Allegheny County or Allegheny County was the location of a transaction or occurrence that took place out of which the cause of action arose.

PATIENTS HAVE OBJECTIVELY REASONABLE EXPECTATIONS OF PRIVACY

20. Plaintiffs are patients of UPMC.

21. As patients of UPMC, Plaintiffs have objectively reasonable expectations of privacy that UPMC, their health care provider, will not disclose their personal information and the content of their communication to third parties without their express authorization.

22. Plaintiffs’ and other patients’ objectively reasonable expectations of privacy in their personal information and communications exchanged with UPMC, their health care provider, are grounded in:

a. UPMC’s status as Plaintiffs’ health care provider;

- b. UPMC'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 and communications;
- d. UPMC's express promises of confidentiality; and
- e. UPMC's implied promises of confidentiality.

UPMC'S DUTIES OF CONFIDENTIALITY

Federal Law

23. 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).

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

25. 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.¹

¹ https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveridentities/De-identification/hhs_deid_guidance.pdf at 5.

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

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

Ancient and Modern Industry Standards of Patient Confidentiality

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

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

29. 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."

30. UPMC requires first year medical students to participate in a white coat ceremony during which they "publicly declare their commitment to integrity, ethical behavior, and honor by reciting the Hippocratic Oath."⁴

31. A medical provider's duty of confidentiality to patients still applies today. In fact,

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

³ Translation of Original Hippocratic Oath by Michael North, National Library of Medicine, National Institutes of Health, https://www.nlm.nih.gov/hmd/greek/greek_oath.html

⁴ Pitt Health Sciences, "Pitt First-Year Medical Students Participate in Annual White Coat Ceremony, Sept. 8, 2018, available: <https://www.upmc.com/media/news/081018-med-school-white-coat>

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

32. 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.

33. AMA Code of Medical Ethics Opinion 3.2.4 provides:

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

34. 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.

Consumer Expectations of Patient Privacy

35. Confidentiality is a cardinal rule of the provider-patient relationship.
36. 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 patients' care.

37. 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.

UPMC’s Express and Implied Promises of Confidentiality

38. UPMC maintains its UPMC.com property and its patient portal at myupmc.upmc.com with knowledge that the property is used by patients to exchange communications with UPMC relating to their providers, treatments, services, and access to a promised “secure” patient portal called MyUPMC.

39. UPMC does not inform patients that their personally identifiable information and the content of their communications at UPMC.com and myupmc.upmc.com are disclosed to Facebook, Google, and numerous other third parties for marketing purposes.

40. UPMC does not obtain any authorization from patients to use their data and communications at UPMC.com for marketing purposes in connection with third parties.

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

42. The UPMC.com property includes three separate privacy statements:

- a. The HIPAA Notice of Privacy Practices;
- b. The MyUPMC terms; and

c. a Privacy Statement.

43. As discussed in more detail below, UPMC makes numerous false or misleading statements about privacy in these three documents.

**HOW UPMC SHARES PATIENT PERSONAL INFORMATION AND
PROCURES THIRD PARTIES TO ACQUIRE
THE CONTENTS OF PATIENT COMMUNICATIONS**

UPMC's Properties

44. UPMC maintains a web property at UPMC.com that is designed for its patients to communicate with it and its entities, including, but not limited to, requesting appointments, paying bills, signing-in to their personal patient portal, and learning more about their conditions, treatments, doctors, and services available from Defendant.

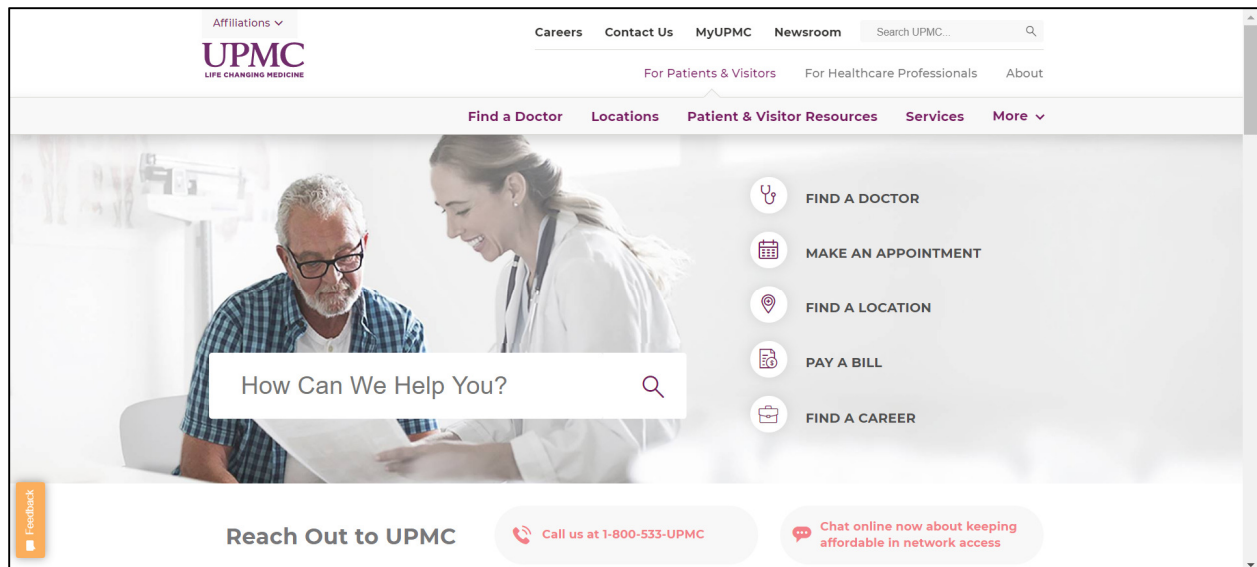
45. UPMC actively encourages patients to use the UPMC.com website.

46. Discharge and appointment paperwork for UPMC patients includes instructions to visit UPMC.com or myupmc.upmc.com to learn more about their providers, conditions, treatments, and personal medical records.

47. UPMC's Notice of Privacy Practices that is provided to all patients instructs, "You can learn more about UPMC at www.upmc.com."

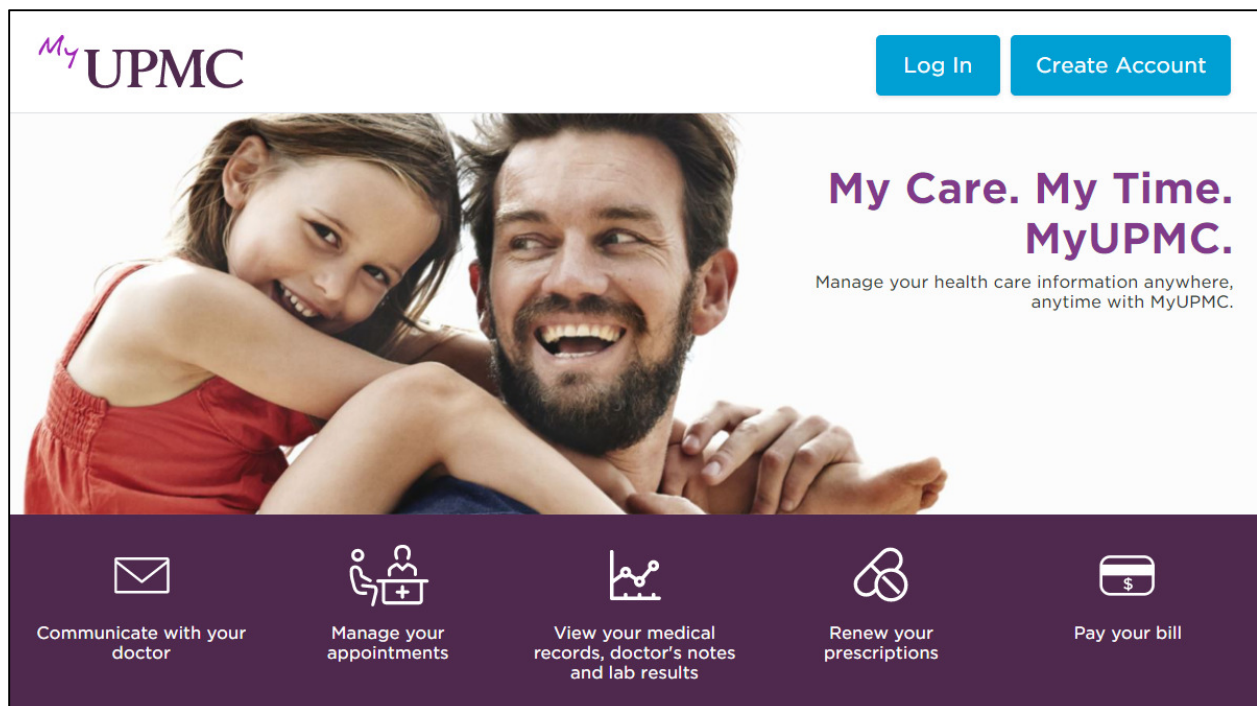
48. Plaintiffs exchanged communications with UPMC at its web property, including www.upmc.com and myupmc.upmc.com.

49. UPMC's homepage shows how the property is designed for use by UPMC patients and potential patients. The homepage provides patients with tools to: "Find a Doctor," "Make an Appointment," "Find a Location," and "Pay Your Bill." It also contains links to access the "MyUPMC" patient health portal.



50. UPMC also maintains a patient portal at the subdomain, myupmc.upmc.com.

51. The sign-in page for MyUPMC appears as such, describing the purpose of the portal to patients as communicating with doctors, managing appointments, viewing medical records, renewing prescriptions, and paying bills:



52. Plaintiffs' communications with Defendant included their sign-up and subsequent log-ins to the "MyUPMC" patient portal Defendant provides to patients at UPMC.com.

Basic Concepts of Internet Communications

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

54. 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.

55. The basic command that web browsers use to communicate with website servers is called a GET request. For example, when a patient types www.upmc.com/services/liver-cancer/conditions/metastatic-colon-cancer into the navigation bar of his or her web browser (or, just as frequently, takes the technological shortcut of clicking a hyperlink), the patient's web browser makes connection with the server for UPMC and sends the following request: "GET /services/liver-cancer/conditions/metastatic-colon-cancer HTTP/1.1."

56. 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.

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

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

59. In some circumstances, the third parties to whom user communications are re-

directed help the website display actual substantive content on the webpage relating to the user communication. For example, the *Pittsburg Post-Gazette* article, “Have an old criminal record? Today, Pennsylvania starts sealing 30M of them automatically” contains this photograph:



Though it appears directly on the *Post-Gazette* website, this photograph is hosted and served by a third-party called Cloudflare through its domain, RackCDN.com.⁵

60. In other cases, the third parties to whom user communications are redirected provide no substantive content relating to the user’s communication. These third parties are typically procured to track user data and communications for marketing purposes.

61. In many such cases, the third party acquires the content of user communications

⁵ The picture from the *Post-Gazette* article can be viewed on its own at the RackCDN domain here: https://9b16f79ca967fd0708d1-2713572fef44aa49ec323e813b06d2d9.ssl.cf2.rackcdn.com/1140x_a10-7_cTC/clean-slate-law-1561719790.jpg.

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 camouflaged to purposefully remain invisible to the user.

62. Without any knowledge, authorization, or action by a user, a web property developer like UPMC's source code can commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the user's personal information and the contents of their communications to third parties.

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

64. 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 they wish to procure to acquire user data and communications. On websites with several third-party trackers, this may cause the page to load more slowly and increases the risk of a coding error effecting functionality and usability. A "tag manager" offers the website developer a vessel 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 for the tag manager. The developer then places the other third-party source code within its account at the tag manager.

65. Google explains the benefits of Google Tag Manager in an Introduction to Google Tag Manager video on YouTube.⁶ 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

⁶ See <https://www.youtube.com/watch?v=KRvbFpeZ11Y>, audio from 0:04 to 1:40.

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](https://www.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.

How UPMC Designs Its Property

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

67. UPMC's Google Tag Manager source code specifically states that it is designed to be invisible. For example, on “metastatic colon cancer” communications page set forth above, the Google Tag Manager source code deployed by UPMC specifies that the “iframe” on the page has a height of 0, a width of 0, display of none, and visibility of hidden.

```
23 <!-- Google Tag Manager -->
24 <noscript><iframe src="//www.googletagmanager.com/ns.html?id=GTM-M77D"
25 height="0" width="0" style="display:none;visibility:hidden"></iframe></noscript>
26 <script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push(
27 {'gtm.start': new Date().getTime(),event:'gtm.js'}
28 );var f=d.getElementsByTagName(s)[0],
29 j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=
30 '//www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);
31 })(window,document,'script','dataLayer','GTM-M77D');</script>
32 <!-- End Google Tag Manager -->
```

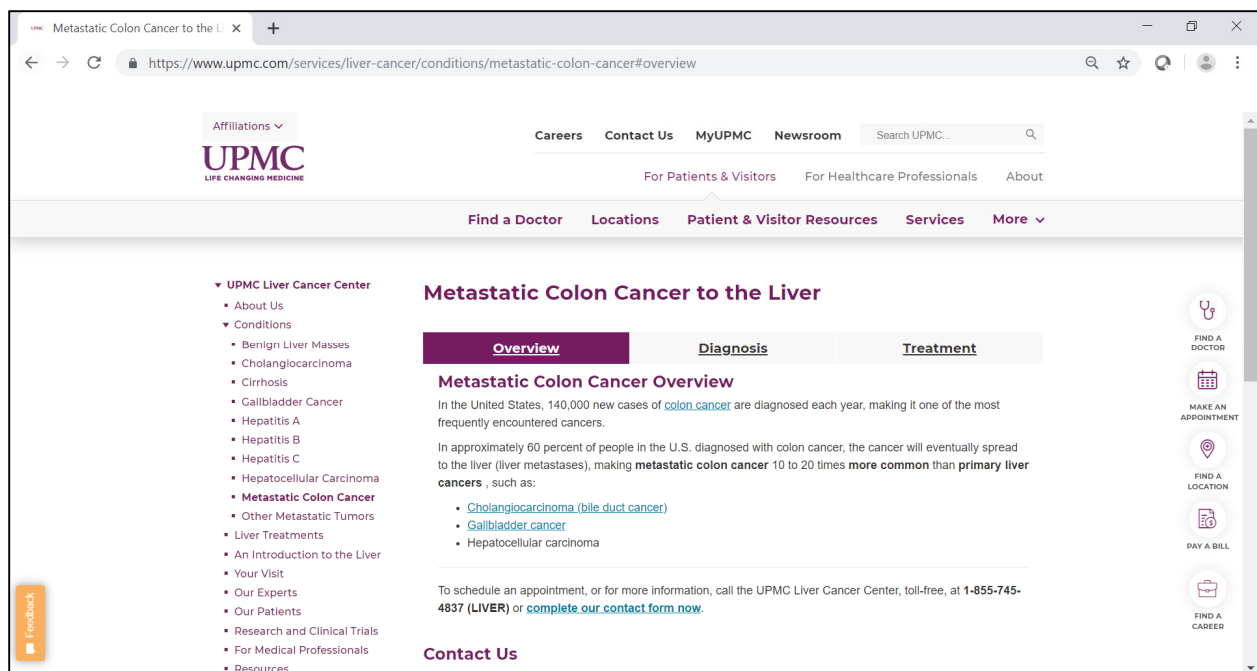
68. UPMC then funnels invisible 1x1 web bugs or pixels through this purposefully invisible iframe to help third parties track, acquire, and record patient data and communications.

69. UPMC places the Google Tag Manager source code in the header of all communications at its property, thereby ensuring that the third-party source code UPMC uses to procure third parties to acquire the content of patient communications is executed before the full content of UPMC’s responsive communications to patients are received by patients on their computing device.

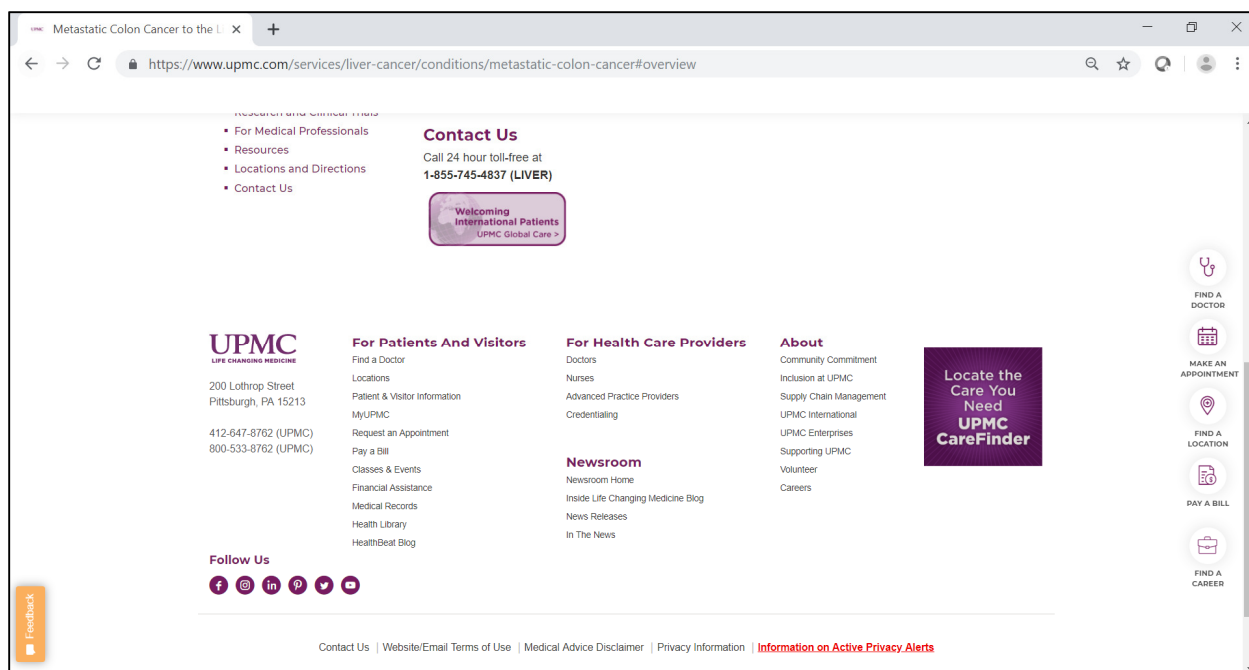
70. For example, on the “Metastatic Colon Cancer” communication page, the Google Tag Manager source code is placed in lines 23 to 32, but the body of UPMC’s return message to the patient does not begin until line 818.

71. None of the tracking is visible to patients on the UPMC website.

72. For example, the “Metastatic Colon Cancer” communication renders as such:



Metastatic Colon Cancer, Screenshot 1



Metastatic Colon Cancer, Screenshot 2

73. Through the third-party source code deployed and invisible web bugs associated with it, UPMC causes patient personally identifiable data and the content of their communications to be re-directed to third parties, including Facebook, Google, Salesforce, Microsoft, and Foresee for marketing purposes.

74. Facebook explains why developers place tag manager and other third-party tracking source code in the header of a return message, before the body. For the Facebook Pixel source code that is deployed by UPMC via Google Tag Manager, Facebook recommends:

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.

75. In addition to placing the Google Tag Manager source code in the header, i.e., before the body of its return communication, UPMC also separately places third-party source code from SiteImprove, Google Remarketing, Decibel Insight, Foresee, and Salesforce in the header.

76. UPMC causes data transmissions and disclosures to be made to different third parties based on the type of communication being exchanged with a patient. For each type of communication listed below, UPMC causes disclosures of personally identifiable information about the patient and the content of their communications to be re-directed to numerous entities without any knowledge, consent, authorization, notification to, or further action of, the patient.

77. UPMC Homepage Communications – On the UPMC homepage at www.upmc.com, UPMC deploys source code that causes patient data and communications to be re-directed (without knowledge, consent, authorization, or any further patient action) to at least nine third-parties: (1) Facebook; (2) Verint Foresee via Answers Cloud; (3) Microsoft via Bing Ads; (4) Brightcove; (5) Crazy Egg; (6) Google via (a) Google DoubleClick, (b) Google DoubleClick Floodlight, (c) Google AdWords, (d) Google Analytics, (e) Google Dynamic Remarketing, and (f) Google Tag Manager; (7) Salesforce via Krux Digital; (8) LivePerson; and (9) SiteImprove.

78. UPMC Find-A-Doctor Communications – On the UPMC Find-a-Doctor page at www.findadoc.upmc.com/FindADocSearch.aspx, UPMC deploys source code that causes patient data and communications to be re-directed (without knowledge, consent, authorization, or any further patient action) to at least 15 third parties: (1) Adobe via (a) Adobe Audience Manager and (b) Adobe Dynamic Tag Management; (2) Aggregate Knowledge; (3) Microsoft via Bing Ads; (4) Oracle via BlueKai; (5) Crazy Egg; (6) Decibel Insight; (7) Google via (a) Google DoubleClick, (b) Google DoubleClick Floodlight, (c) Google DoubleClick Spotlight, (d) Google AdWords, (e)

Google Analytics, (f) Google Dynamic Remarketing, and (g) Google Tag Manager; (8) Facebook via (a) Facebook Connect, (b) Facebook Custom Audience, and (c) Facebook Tracking Pixel; (9) Verint Foresee via Foresee; (10) FullStory; (11) LivePerson; (12) LiveRamp; (13) SiteImprove; (14) TradeDesk; and (15) Undertone.

79. UPMC Find-A-Doctor Search Result Communications – On the UPMC Find-a-Doctor search result communications pages, UPMC deploys source code that causes patient data and communications to be re-directed (without knowledge, consent, authorization, or any further patient action) to at least 10 third parties: (1) Adobe via (a) Adobe Audience Manager, and (b) Adobe Dynamic Tag Management; (2) Microsoft via Bing Ads; (3) Crazy Egg; (4) Decibel Insight; (5) Google via (a) Google DoubleClick, (b) Google DoubleClick Floodlight, (c) Google DoubleClick Spotlight, (d) Google AdWords, (e) Google Analytics, (f) Google Dynamic Remarketing, and (g) Google Tag Manager; (6) Facebook via (a) Facebook Custom Audience, and (b) Facebook Tracking Pixel; (7) Verint Foresee via ForeSee; (8) FullStory; (9) LivePerson; and (10) SiteImprove.

80. UPMC Doctor Pages Communications – On UPMC physician pages, such as <http://findadoc.upmc.com/PhysicianBioQuery.aspx?EPCDID=172377&hosp=0>,⁷ UPMC deploys source code that causes patient data and communications to be re-directed (without knowledge, consent, authorization, or any further patient action) to at least 10 third parties: (1) Adobe via (a) Adobe Audience Manager, and (b) Adobe Dynamic Tag Management; (2) Microsoft via Bing Ads;

⁷ UPMC's URL naming convention for doctor profile pages gives each physician a unique persistent "EPCDID." Although it does not directly reveal a doctor's name, such can be discovered simply by typing the URL or copy-pasting it into the navigation bar of a search engine. 172377 is the EPCDID for Dr. Jessica Layne Berger, a gynecologist. Further, although the URL is coded, as explained below, UPMC's source code causes disclosure of each physician's name, on its own, to third-parties when patients exchange communications on a physician profile page.

(3) Crazy Egg; (4) Decibel Insight; (5) Google via (a) Google DoubleClick, (b) Google DoubleClick Floodlight, (c) Google DoubleClick Spotlight, (d) Google AdWords, (e) Google Analytics, (f) Google Dynamic Remarketing, and (g) Google Tag Manager; (6) Verint Foresee via ForeSee; (7) FullStory; (8) LivePerson; (9) SiteImprove; and (10) Salesforce via Krux Digital.

81. UPMC Medical Conditions Communications – For UPMC medical conditions communications, i.e., www.upmc.com/services/liver-cancer/conditions/metastatic-colon-cancer, UPMC deploys source code that causes patient data and communications to be re-directed (without knowledge, consent, authorization, or any further patient action) to at least six third parties: (1) Verint Foresee via Answers Cloud; (2) Microsoft via Bing Ads; (3) Crazy Egg; (4) Google via (a) Google Analytics Audiences, (b) Google Analytics, (c) Google Dynamic Remarketing, and (d) Google Tag Manager; (5) Salesforce via Krux Digital; and (6) SiteImprove.

82. UPMC Medical Appointments Communications – On UPMC medical appointments communications pages, i.e. <https://www.upmc.com/contact/appointment-request>, UPMC deploys source code that causes patient data and communications to be re-directed (without knowledge, consent, authorization, or any further patient action) to at least eight third parties: (1) Adobe via (a) Adobe Audience Manager, and (b) Adobe Dynamic Tag Management; (2) Verint Foresee via Answers Cloud; (3) Microsoft via Bing Ads; (4) Crazy Egg; (5) Decibel Insight; (6) Google via (a) Google DoubleClick, (b) Google DoubleClick Floodlight, (c) Google DoubleClick Spotlight, (d) Google AdWords, (e) Google Analytics, (f) Google Dynamic Remarketing, and (g) Google Tag Manager; (7) Salesforce via Krux Digital; and (8) SiteImprove.

83. UPMC Patient Portal Log-In Page Communications – On the UPMC Patient Portal log-in communications page at <https://myupmc.upmc.com>, UPMC deploys source code that causes patient data and communications to be re-directed (without knowledge, consent,

authorization, or any further patient action) to at least three third parties: (1) Google via (a) Google DoubleClick, (b) Google DoubleClick Floodlight, (c) Google DoubleClick AdExchange, (d) Google AdWords, (e) Google Analytics, (f) Google Dynamic Remarketing, and (g) Google Tag Manager, (2) Facebook via (a) Facebook Connect, (b) Facebook Custom Audience, and (c) Facebook Tracking Pixel; and (3) Kenshoo.

84. UPMC Patient Portal Communications – For patient communications exchanged entirely within the UPMC Patient Portal, UPMC deploys source code that causes patient data and communications to be re-directed (without knowledge, consent, authorization, or any further patient action) to at least two third parties: (1) Google via (a) Google DoubleClick and (b) Google Analytics; and (2) LivePerson.

85. Disclosures While a Patient is Logged-In to the Patient Portal – Once logged-in to MyUPMC, a patient is provided with several options to learn more information about their care (including their providers, conditions, treatments, and UPMC services) through hyperlinks that UPMC places inside the MyUPMC portal. When a patient clicks on a hyperlink inside MyUPMC to exchange communications about such topics, UPMC's source code commands the patient's communications device to open new windows through which UPMC re-directs the patients' personal information and the content of their communications via invisible web pixels as described above. Thus, by design, rather than protecting the confidentiality of patient communications while they are signed-in to MyUPMC, Defendants instead funnels patients' personal information and the contents of their communications to third parties. The third parties to whom such data and content are disclosed is determined by the type of communication that the patient sent within the portal. For example, a communication about a particular doctor would cause the disclosures explained above in the "Doctor Pages" paragraph.

86. UPMC Patient Portal Communication Disclosures to Facebook – Upon information and belief as further described below, the Google DoubleClick source code that UPMC deploys wholly within the patient portal is a conduit through which UPMC makes further disclosures of patient personally identifiable information to Facebook.

The Content UPMC Procures Third Parties to Intercept

87. In most cases of patient communications at UPMC.com, UPMC causes the disclosure the particular content of a patient’s communication at the UPMC.com website to third-parties by re-directing an exact copy of the GET request that the patient sent to UPMC.

88. For example, consider the “metastatic colon cancer” communication:

- a. When a patient sends a communication to request information about “metastatic colon cancer,” the GET request sent from the patient’s browser to UPMC is ‘GET services/liver-cancer/conditions/metastatic-colon-cancer,’ the responsive communication from UPMC is a short overview of “metastatic colon cancer,” and the URL of the webpage to which the patient is directed is www.upmc.com/services/liver-cancer/conditions/metastatic-colon-cancer.
- b. When a user clicks their mouse to exchange the “Metastatic Colon Cancer” communication with UPMC, its source code causes an exact replica to be re-directed to several third parties in separate, contemporaneous data transmissions. For Google Doubleclick, UPMC causes the disclosure of the following information in a GET request to Google:

Request Headers	[Raw] [Header Definitions]
GET /pagead/viewthroughconversion/1065944505/?random=1561918472642&cv=9&fst=1561918472642&num=1&label=yESqCOFFjQQQuYuk_AM&guid=ON&resp=GooglemKTybQhCsO&u_h=1080&u_w=1920&u_ah=1040&u_aw=1920&u_cd=24&u_his=2&u_tz=-300&u_java=false&u_nplug=3&u_nmime=4>m=2wg6k2&sendb=1&frm=0&url=https%3A%2F%2Fwww.upmc.com%2Fservices%2Fliver-cancer%2Fconditions%2Fmetastatic-colon-cancer&tiba=Metastatic%20Colon%20Cancer%20to%20the%20Liver%20Symptoms%20%26%20Treatment%20%7C%20UPMC&async=1&rfmt=3&fmt=4 HTTP/1.1	

c. UPMC also causes disclosure of the precise content of the patient communication to Google through a “referrer header,” an optional data field that identifies the address of the webpage, in this example, www.upmc.com/services/liver-cancer/conditions/metastatic-colon-cancer, which contains within it an exact replica of the GET request sent from the patient to UPMC and information relating to UPMC’s response.

89. UPMC’s source code at the Metastatic Cancer communications page illustrates this point because UPMC refers to the type of data disclosed as content:

```
94 <link rel="canonical" itemprop="url" href="https://www.upmc.com/services/liver-cancer/conditions/metastatic-colon-cancer" />
95 <meta content="https://www.upmc.com/services/liver-cancer/conditions/metastatic-colon-cancer" property="og:url" />
96 <meta name="author" content="">
97 <meta property="og:type" content="article" />
98 <meta content="Metastatic Colon Cancer to the Liver Symptoms & Treatment | UPMC" property="og:title" />
99 <meta content="Learn more about the symptoms and diagnosis of metastatic colon cancer to the liver, and find more information about
100 treatment options." property="og:description" />
101 <meta name="description" content="Learn more about the symptoms and diagnosis of metastatic colon cancer to the liver, and find more
information about treatment options." />
102 <link rel="stylesheet" href="/Presentation/includes/Modules/FontAwesome/4.3.0/css/font-awesome.min.css" /> <meta name="google-site-
verification" content="7i5vgy7UPjQKFhXUD8mLi_jq5DaaqEkiK-D-K4Bs0rQ" />
<meta property="og:image" content="https://www.upmc.com/-/media/upmc/logos/upmc_logo_og.jpg?la=en" />
```

90. In a limited number of cases, UPMC masks the content of the patient communication. For example, on the “Find-A-Doctor” page, if a patient conducts a search for Dr. Berger, the fact that they have searched for “Berger” is sent in a secure POST communication to UPMC, and the GET requests and referrer headers for the search results page that re-directed to third parties are encrypted, with phrases such as “Safe Session Key” and “Safe Session.”

91. The results for the “Berger” search reveal two doctors in the UPMC system named Berger. The first result for the “Berger” search is Dr. Jessica Layne Berger, a gynecologist. The results page for the Berger search is:

UPMC LIFE CHANGING MEDICINE

MyUPMC Find a Doctor Careers Resources

For Patients, Families & Visitors For Health Care Professionals About UPMC

Find a Doctor

To speak with an appointment scheduler, call **1-800-533-UPMC** between 7 a.m. and 7 p.m. Monday through Friday.

Note: We can schedule appointments for many — but not all — UPMC doctors and locations at this number.

UPMC Overall Patient Satisfaction Rating **4.8 out of 5** 490,819 Reviews

SEARCH FOR A UPMC DOCTOR NEAR YOU

Search Results (3)

<< First < Prev **Page 1 of 1** Next > Last >>

DOCTOR
Jessica Layne Berger, MD
Specialty:
 Gynecology
Sub Specialty:
 Gynecologic Oncology
Patient Satisfaction Ratings:
 4.9 Stars
 165 Patient Satisfaction Ratings
[115 Comments](#)
[Learn About Our Survey](#)

Magee Gynecologic Cancer Program
 UPMC Passavant - McCandless
 9100 Babcock Blvd.
 Pittsburgh, PA 15237
Office Phone:
 (412) 748-6454
Map
 UPMC Magee-Womens Hospital
 300 Halket St.
 Suite 1750
 Pittsburgh, PA 15213
Office Phone:
 (412) 641-5411
Map
 UPMC Hamot Womens Specialty Care Center
 Erie - Magee-Womens Hospital
 440 East 9th St.

[View Full Profile](#)

[Appointment Information](#)

92. Although UPMC makes efforts to encrypt patient search terms at the precise moment when they are made, the encryption is abandoned when a patient clicks to “View Full Profile” of any doctor within a search result. Here, when a patient clicks to view the full profile of Dr. Jessica Berger, UPMC source code causes disclosure of the content of that communication to at least eight third parties: (1) Adobe, (2) Microsoft, (3) Crazy Egg, (4) Google, (5) Foresee, (6) Salesforce, (7) LivePerson, and (8) SiteImprove. For Google, UPMC causes the following data to be transmitted to Google contemporaneous to the communication exchanged with the patient:

utmdt	Jessica Layne Berger, MD - Find A Doctor, UPMC
utmhid	237082073
utmr	0
utmp	/PhysicianBioQuery.aspx?EPCDID=172377&hosp=0
utmpg	1:FindADoc

93. UPMC's encryption of the particular content of the search query illustrates that it is not necessary for Defendant to disclose the content of patient communications at its property.

The Continual Nature of HTTP and HTTPs Communications through Packet-Switching

94. Modern communications work through a process called packet-switching, a concise explanation of which can be found in *U.S. v. Szymuszkiewicz*, 622 F.3d 701, 704 (7th Cir. 2010):

When the Wiretap Act was enacted in 1968, the normal communications pathway was circuit switching: the telephone company's machinery (initially switchboards, then mechanical solenoids, and finally computers) would establish a single electronic pathway, or circuit, between one telephone and another. Computers can communicate over dedicated circuits, but usually they break each message into packets, which can be routed over a network without the need to dedicate a whole circuit to a single message.

Each packet contains some of the message's content, plus information about the packet's destination. Each packet travels independently, moving from router to router within a network to find a path toward the ultimate destination. The Wikipedia entry on packet-switched networks contains a helpful description, plus citations to technical references. The routers, and the computers on both ends, arrange the packets (and their address information), and resend as necessary, so that at least one copy of each of the message's many packets reaches its goal. Lost packets can be repeated, and a whole message can be transmitted by sending each packet through a different route. Every packet may go by a different route. Only at the end are the pieces put back together and an intelligible communication formed. The path of any particular packet, and the order in which it arrives at the end, is irrelevant to the success of the communication. Computers use a recipe known as a protocol that enables them to agree on how packets are formatted and reassembled.

95. Packet-switching technology is now widespread. For example, all 4G and 5G voice or data communications are made via packet-switching technology.

96. The protocol for communications that occur through a web browser is called HTTP or HTTPS. HTTP stands for “Hypertext Transfer Protocol” and HTTPS stands for “Hypertext Transfer Protocol Secure.” HTTPS communications are typically encrypted using either Transport Layer Security (“TLS”) or Secure Sockets Layer (“SSL”).

97. When two Internet users (for example Jane Doe I and UPMC) communicate using HTTP or HTTPS, the communication starts with Jane Doe I clicking on a hyperlink or typing the web address into her browser and hitting Enter. Immediately upon Jane Doe I clicking the hyperlink or hitting Enter, her web browser reads the domain name of the recipient (here, UPMC.com), translates it into the recipient’s IP address (here, 157.229.38.48), and initiates a communication exchange by sending a request to the destination IP address to establish a connection between the browser and UPMC’s server.

98. Once a connection is established between the devices (browser and server), the browser transmits the precise content of Jane Doe I’s communication to UPMC, requesting that UPMC exchange information on the topic of her communication.

99. Jane Doe I’s browser and UPMC’s web server then begin the packet-switching process, with thousands of data transmissions being made between her browser and UPMC’s web server over a very short period of time.

100. With some Internet communications, the packet-switching process between a sender and receiver occurs in a single direction. For example, in an email communication, the sender’s communication is sent in hundreds or thousands of individual packets, and soon thereafter arrives at the recipient’s email server. When that email arrives at the recipient’s email server, it is complete because an email is a one-way communication and there is no ongoing connection made between the browser of the email sender and the server of the email recipient.

101. HTTP and HTTPS communications between patients and UPMC are bilateral and ongoing, much like a telephone conversation. Once the initial conversation is made (sometimes called a “handshake”), the communication commences and continues between the parties in a bilateral fashion until the patient leaves UPMC’s property.

102. When a developer deploys third-party tracking tools, the source code commands the web browser to re-direct the contents of a user’s HTTP or HTTPS communication and the website’s responses to third parties in the middle of the bilateral, ongoing communications session between the user and the website.

The Forms of Patient Personally Identifiable Information that UPMC Uses to Procure Third Parties to Acquire the Content of Patient Communications

103. UPMC’s source code causes transmission of the content of patient communications and the following personally identifiable information and personal identifiers to third parties:

- a. Patient IP addresses;
- b. Unique, persistent patient cookie identifiers; and
- c. Browser-fingerprints.

104. UPMC shares and uses these patient identifiers without patient knowledge, consent, authorization, or any further action by the patient to, among other things:

- a. Procure and help the third parties to acquire the content of patient communications for marketing purposes;
- b. Disclose patient medical data and communications to the third parties;
- c. Violate provider-patient confidentiality; and
- d. Engage in unfair and deceptive trade practices.

Patient IP Addresses are Personally Identifiable

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

106. IP addresses are used to identify and route communications on the Internet.
107. IP addresses of individual Internet users are used by Internet service providers, websites, and third-party tracking companies to facilitate and track Internet communications.
108. Facebook tracks every IP address ever associated with a Facebook user.
109. Google tracks IP addresses associated with specific Internet users.
110. The other third-party marketing companies that UPMC procured to obtain the contents of patient communications associate particular IP addresses with specific Internet users.
111. Individual homes and their occupants can be, and are, tracked and targeted with advertising using IP addresses.
112. Under HIPAA, an IP address is considered personally identifiable information. *See* 45 C.F.R. § 164.514(b)(2)(i)(O).
113. UPMC uses and causes the disclosure of patient IP addresses to third parties with each re-directed communication described herein, including patient communications within the MyUPMC Patient Portal and on the Patient Portal log-in page, and communications concerning individual providers, conditions, and treatments.

Internet Cookies are Personally Identifiable

114. 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.
115. Computer programmers eventually developed ‘cookies’ – small text files that web servers can place on a person’s web browser and computing device when that person’s web

browser interacts with the website server. Some cookies are designed to acquire and record an individual Internet user's communications and activities on websites across the Internet.

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

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

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

119. 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."

120. 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, UPMC sets a collection of its own cookies on patients' browsers when they visit any web page on the UPMC website. First-party cookies can be helpful to the user, server, and/or website to assist with security, log in, and functionality.

- b. “Third-party cookies” are set on a user’s device by website servers other than the website or server with which the user is exchanging communications. For example, the same patient who visits UPMC 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.

121. 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.

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

UPMC’s Cookie Synching with Facebook and Google

123. Based on an Internet security policy known as same-origin policy, web browsers prevent different entities from accessing each other’s cookies. For example, Facebook would be prevented from obtaining UPMC cookies and vice-versa by way of the same-origin policy. Similarly, Facebook cookies could not be set or accessed via another website’s domain.

124. However, Javascript source code running in a webpage can bypass the same-origin policy to send a putative “first-party” cookie value in a tracking pixel to a third-party entity. This technique is known in the Internet advertising business as “cookie synching.”

125. Cookie synching allows cooperating websites to learn each other’s cookie identification numbers for the same user. Once the cookie synching operation is complete, the two websites exchange information that they have collected and hold about a user (or a patient in the case of UPMC).

126. In effect, cookie synching is a method through which Facebook, Google, and other third-party marketing companies set and access third-party cookies that masquerade as first-party cookies. By designing these special third-party cookies that are set by first-party websites, Facebook and Google hack their way around any cookie blockers that users set up to stop their tracking.

127. The Facebook cookie used for cookie synching is named _fbp.

128. Google has several cookies used for this purpose, including, but not limited to: _gid, _ga, _utma, and _utmz.

129. UPMC engages in cookie synching with Facebook, Google, and others.

130. UPMC uses and causes the disclosure of patient cookie identifiers through cookie synching technologies with each re-directed communication described herein, including patient communications within the Patient Portal and on the patient-portal log-in page, and communications concerning individual providers, conditions, and treatments.

Browser-Fingerprints are Personally Identifiable

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

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

133. 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.⁸

134. Google recently explained, "With fingerprinting, developers have found ways to use tiny bits of information that vary between users, such as what device they have or what fonts they have installed to generate a unique identifier which can then be used to match a user across websites. Unlike cookies, users cannot clear their fingerprint, and therefore cannot control how their information is collected."⁹

135. In 2017, researchers showed that browser fingerprinting techniques can successfully identify 99.24 percent of users.¹⁰

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

⁸ Katarzyna Szymielewicz and Bill Dudington, Electronic Frontier Foundation, The GDPR and Browser Fingerprinting: How It Changes the Game for the Sneakiest Web Trackers, <https://www.eff.org/deeplinks/2018/06/gdpr-and-browser-fingerprinting-how-it-changes-game-sneakiest-web-trackers>.

⁹ <https://www.blog.google/products/chrome/building-a-more-private-web/>

¹⁰ Yinzhao Cao, Song Li, Erik Wijmans, (Cross-)Browser Fingerprinting via OS and Hardware Level Features, Proceedings of the Network and Distributed Security Symposium, March 2017, available at http://yinzhaocao.org/TrackingFree/crossbrowsertracking_NDSS17.pdf.

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

UPMC's Disclosures Must Be Considered Individually and As a Whole

138. Each of the individual data elements described above is personally identifiable on their own. However, UPMC's disclosures of such personally identifiable data elements do not occur in a vacuum. The disclosures of the different data elements are tied together and, when taken together, these data elements are even more accurate in identifying individual patients, particularly when disclosed to data companies such as Facebook, Google, and others that expressly state they use such data elements to identify individuals.

UPMC'S DISCLOSURES ARE NOT PUBLIC INFORMATION

139. The www.UPMC.com web property is publicly available to patients, potential patients, and other Internet users just as UPMC hospitals are publicly available.

140. The fact that Plaintiffs are patients of UPMC is not publicly available.

141. The fact that Plaintiffs exchange communications with UPMC at its web property is not publicly available.

142. The facts that Plaintiffs have registered for, used, and exchanged communications with UPMC inside the MyUPMC patient portal, and the specific data and times associated with those communications, are not publicly available.

143. The specific communications exchanged between Plaintiffs and UPMC, including

communications about specific providers, conditions and treatments, are not publicly available information – regardless of whether such communications occurred before or after Plaintiffs or patients had signed in to MyUPMC.

144. The personal information that UPMC causes to be disclosed to third parties about patients after they have signed in to the MyUPMC portal is not public information.

UPMC’S DISCLOSURES ARE NOT NECESSARY

145. None of the third-party marketing disclosures described herein are necessary for UPMC to maintain a web property, MyUPMC, or to utilize social media marketing tools.

146. It is possible for UPMC to provide a patient portal without making any disclosures about patient sign-ins, log-outs, or other communications while they are signed in, to the MyUPMC portal, to Google, Facebook, or any other third party.

147. Despite these possibilities, UPMC willfully chose to disclose personally identifiable patient data and communications to several third-party marketing companies.

148. It is not necessary that the content of a user’s communication be shared with third-party tracking companies. In fact, it is possible for companies to utilize third-party tracking tools without disclosing either the specific contents of communications or a user’s status as a patient of a health care provider.

UPMC IS ENRICHED FOR MAKING THE UNAUTHORIZED DISCLOSURES

149. The purpose of UPMC’s disclosures and procurement of third parties to intercept patient communications is marketing.

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

151. This barter transaction between UPMC and the third parties constitutes a sale.

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

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

154. Once the personally identifiable data relating to patient communications is disclosed to third parties, UPMC loses the ability to control its further dissemination and use. As described below, several of the third parties share and use data with fourth parties and use data collected from websites such as UPMC to sell marketing products to others.

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

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

157. Retargeting enables UPMC to show advertisements on other websites to patients or potential patients based on specific communications exchanged at UPMC's property. Using the Facebook Pixel, UPMC can target ads on Facebook itself or the Facebook advertising network to patients for whom Facebook recorded actions at UPMC. The same or similar targeted actions can be accomplished via disclosures to the other third-party marketing companies.

158. In addition to enabling UPMC to advertise to patients and potential patients on

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

159. The Trade Desk, a third party to whom UPMC makes disclosures, explains, "Reaching the right customers at the right time is a priority for any marketer. But there are only so many opportunities to target your messaging on a single device. ... Our cross-device targeting tools match multiple devices and channels to a unique ID, so you can serve up relevant ads when and where they'll be most impactful."

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

161. UPMC's use of cross-device targeting illustrates that the data elements it discloses to the third parties are personally identifiable because they enable the tracking of patients across the multiple devices that the patient owns, even when the patient has never communicated with Defendant on one or more of their devices.

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

163. UPMC obtains additional revenue from its deployment of third-party tracking tools

through which it discloses personally identifiable patient data and communications to third parties.

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

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

The Value of the Data UPMC Discloses

166. The monetization of the data disclosed by UPMC demonstrates the inherent value of such information.

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

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

169. Personal information is now viewed as a form of currency and a corporate asset.

Professor Paul M. Schwartz has noted in the *Harvard Law Review*:

Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.

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

171. For example, one 2015 study determined that Americans place more value on their “health condition” than any other piece of data about them, with a minimum value of \$82.90.¹¹ By comparison, respondents assigned a value of \$67.00 to their passwords, \$55.70 to their Social Security number, and \$40.10 to their credit history.

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

173. Even with strict restrictions on the disclosure of personally identifiable health information, a robust market exists for the trade of de-identified health data.¹²

174. UPMC’s disclosures violate Plaintiffs’ and other patients’ privacy rights not to have their personally identifiable patient data and communications disclosed without their knowledge, authorization, consent, or any further action on their part.

175. UPMC’s disclosures violate Plaintiffs’ and other patients’ legally enforceable and valuable property rights to determine how their personally identifiable health data and the content of their communications exchanged with their health care providers is used and to determine to whom such data may be disclosed and benefit.

¹¹ Ponemon Institute, Privacy and Security in a Connected Life: A Study of US Consumers, March 2015, available at <https://www.trendmicro.de/media/report/ponemon-privacy-and-security-in-a-connected-life-us-consumers-report-en.pdf>.

¹² See How Data Brokers Make Money Off Your Medical Records, Scientific American, <https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/>; Your Private Medical Data is for Sale – and It’s Driving a Business Worth Billions, The Guardian, <https://www.theguardian.com/technology/2017/jan/10/medical-data-multibillion-dollar-business-report-warns>; The Hidden Global Trade in Patient Medical Data, YaleGlobal Online, <https://yaleglobal.yale.edu/content/hidden-global-trade-patient-medical-data>.

**PATIENTS HAVE A PROTECTABLE PROPERTY INTEREST IN THEIR
PERSONALLY IDENTIFIABLE DATA AND COMMUNICATIONS WITH UPMC**

176. Property is the right of any person to possess, use, enjoy, or dispose of a thing, including intangible things such as data or communications.

177. The Pennsylvania Supreme Court has defined property:

‘Property’ has been thus defined: ‘In law it is not the physical material object which constitutes property. The term means something more than the mere thing which a person owns[.] The idea of property springs out of the connection, or control, or interest, which, according to law, may be acquired in or over things.

In modern legal systems, property includes practically all valuable rights, the term being indicative and descriptive of every possible interest which a person can have, in any and every thing that is the subject of ownership by man, including every valuable interest which can be enjoyed as property, and recognized as such, and extending to every species of valuable right or interest in either real or personal property, or in easements, franchises, and incorporeal hereditaments.

Schuster v. Pennsylvania Turnpike Commission, 395 Pa. 441, 453 (1959), citing 73 C.J.S. Property §1b at 138-40.

178. Property includes intangible data.

179. Patient lists are property.

180. Federal and state law grants patients the rights to:

- a. protect the confidentiality of data that identifies them as a patient of a particular health care provider; and
- b. restrict the use of their health data, including their status as a patient, to only those uses related to their care or otherwise authorized by state or federal law in the absence of patient authorization.

181. Patient rights to protect their confidentiality and restrict the use of their health data is a valuable right, as described herein.

182. In addition to property rights as patients, Plaintiff enjoys property rights in the privacy of the content of her communications.

183. American courts have long recognized common law property rights in the content of a person's communications that are not to be used or disclosed to others without authorization.

184. Plaintiff and other patients possess further property rights against unauthorized dissemination and use of the contents of their communications through the Pennsylvania Wiretapping and Electronic Surveillance Control Act.

185. Plaintiff and other patients possess further property rights against unauthorized use of their personal identifiers through 42 Pa.C.S. § 8315.

THE THIRD PARTIES TO WHOM UPMC MAKES DISCLOSURES

Google

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

187. 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."¹³

¹³ *Who Has More of Your Personal Data than Facebook? Try Google*, *The Wall Street Journal*, <https://www.wsj.com/articles/who-has-more-of-your-personal-data-than-facebook-try-google-1524398401>.

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

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

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

191. UPMC deploys the Google Remarketing source code directly on the UPMC website on at least one page: the “Metastatic Colon Cancer” communications page set forth above.

192. As deployed on the “Metastatic Colon Cancer” communications page, the Google code specifically warns developers that Google “[r]emarketing tags may not be associated with personally identifiable information or placed on pages related to sensitive categories,” such as health.

```
46 //-- Google Code for Remarketing tag -->
47 //-- Remarketing tags may not be associated with personally identifiable information or placed on
   pages related to sensitive categories. For instructions on adding this tag and more information on
   the above requirements, read the setup guide: google.com/ads/remarketingsetup -->
48 var google_conversion_id = 1065944505;
49 var google_conversion_label = "yESqC0FFjQQQuYuk_AM";
50 var google_custom_params = window.google_tag_params;
51 var google_remarketing_only = true;
52 </script>
```

193. By following the instructions in the Google source code, a developer is warned that “Health in personalized advertising” is a “Prohibited category” for Google’s personalized advertising tools. Specifically, Google’s advertising policies page states:¹⁴

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. ...

¹⁴ <https://support.google.com/adspolicy/answer/143465?hl=en>

You aren't allowed to do the following:

✗ Collect information related to sensitive interest categories (see [Personalized advertising policy principles](#) below for more about sensitive interest categories)

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

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

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

195. Google provides instructions for web developers to anonymize IP addresses when they use Google Analytics.¹⁵ Google explains that the IP anonymization feature “is designed to help site owners comply with their own privacy policies, or, in some countries, recommendations from local data protection authorities, which may prevent the storage of full IP address information.” The Google IP anonymization instructions tell web developers to add a parameter

¹⁵ Available at <https://support.google.com/analytics/answer/2763052?hl=en>

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.’

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

197. Although Google Analytics is promoted primarily as a tool to measure demographics statistics about website usage, it can also be used for advertising known as ‘remarketing’ – the practice of directed targeted ads to users who have previously taken a certain action that the developer or marketer believes makes them more likely to convert into a paying customer. “Remarketing” is the name for the process that enables a retailer to follow users around the Internet with specific ads related to the products or services that the user recently viewed.

198. Google explains how re-marketing with Google Analytics works:¹⁶

About remarketing audiences in Analytics

Re-engage audiences that are likely to convert.

A remarketing audience is a list of cookies or mobile-advertising IDs that represents a group of users you want to re-engage because of their likelihood to [convert](#). You create remarketing audiences based on user behavior on your site or app, and then use those audiences as the basis for remarketing campaigns in your ad accounts like Google Ads and Display & Video 360.

199. When a developer enables Google Analytics’ re-marketing, the source code deployed causes transmissions of personal identifiers and the content of user communications to Google DoubleClick through the domain, stats.g.doubleclick.net.

¹⁶ See <https://support.google.com/analytics/answer/2611268?hl=en&topic=2611283>

200. UPMC has enabled Google Analytics' re-marketing, thereby causing such disclosures to stats.g.doubleclick.net.

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

- a. while logged in to the Patient Portal at MyUPMC;
- b. on the patient portal log-in page at MyUPMC; and
- c. at UPMC.com that pertain to the patient's communications regarding specific providers, conditions, treatments, and appointment requests.

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

203. The Google Analytics remarketing function causes the transmission of several cookie identifiers to Google DoubleClick, including a cookie called 'fbp.'

204. Upon information and belief, this enables UPMC to disclose patient status and communications (made both inside and outside the patient portal) to Facebook at a later time.

Facebook

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

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

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

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

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

210. The Facebook Pixel, a product for Facebook Business, is a “piece of code” that lets developers “measure, optimize, and build audiences for ... ad campaigns.”¹⁷

211. Key features of the Facebook Pixel include its ability to help developers:

- a. “Measure cross-device conversions” and “understand how your cross-device ads help influence conversion”;
- b. “Optimize delivery to people likely to take action” and “ensure your ads are shown to the people most likely to take action”; and
- c. “Create custom audiences from website visitors” and create “dynamic ads [to] help you automatically show website visitors the products they viewed on your website – or related ones.”

212. The Facebook Pixel is an invisible 1x1 web bug.

213. 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.”

¹⁷ <https://www.facebook.com/business/learn/facebook-ads-pixel>

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.

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

How the Facebook pixel works

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

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

Installing The Pixel

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

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

216. UPMC has installed the Facebook Tracking Pixel on its Patient Portal login page at myupmc.upmc.com.

217. When a patient visits the Patient Portal login page, UPMC uses the patient's personal identifiers by causing the identifiers to be transmitted to Facebook along with the fact that the patient has exchanged a communication at the UPMC patient portal log-in page.

218. The specific means of identification that UPMC uses to help Facebook acquire and record patient communications at the UPMC patient portal log-in page include the patient's IP address and cookie values, including Facebook cookies set by UPMC through cookie synching.

219. Through the source code deployed by UPMC, the cookies that Defendant uses to help Facebook identify patients include, but are not necessarily limited to, cookies named: c_user, datr, fr, and fbp.

220. 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.

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

222. 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.¹⁸

223. The datr cookie identifies a patient's specific web browser from which the patient is sending the communication. It is an identifier that is unique to the patient's specific web browser

¹⁸ For example, Jackie Gelzheiser, the Director of Marketing and Communications at UPMC Enterprises, has a Facebook user profile with a c_user cookie value ending with the digits 3486. Plaintiffs' counsel possesses, but chooses not to disclose, the full value in a public document.

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.

224. The fr cookie is a Facebook identifier that is an encrypted combination of the c_user and datr cookies.¹⁹

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

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

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

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

229. According to Facebook, "adequate consent" means UPMC must make "appropriate disclosures ... [t]hat third parties, including Facebook, may use cookies, web beacons, and other ... technologies to ... receive information from" UPMC. Facebook Platform Policy at ¶ 2.8. In

¹⁹ See Facebook Tracking Through Social Plug-ins: Technical Report prepared for the Belgian Privacy Commission, Mar. 27, 2015, available at https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf.

another provision, Facebook instructs developers to provide “robust and sufficient prominent notice” everywhere that the Facebook Pixel is used. Facebook Business Tools Terms at ¶ 3.

230. UPMC fails to follow Facebook’s standards for obtaining consent.

231. Upon information and belief, Defendant has also deployed Facebook source code to help UPMC disclose to Facebook the actions that patients take within the Patient Portal.

232. Facebook provides developers with instructions on how to integrate the Facebook Tracking Pixel with Google tracking technologies, specifically the DoubleClick Campaign Manager.

233. There is another separate ‘fbp’ cookie that UPMC causes to be created and transmitted to Google DoubleClick on the UPMC Patient Portal.

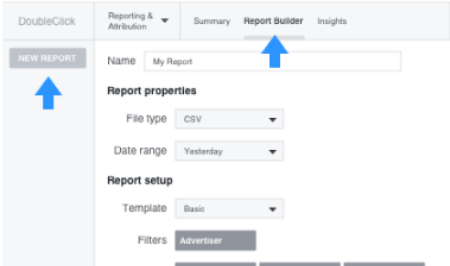
234. Upon information and belief, the existence of source code that causes the creation and transmission of an ‘fbp’ cookie identifier to Google DoubleClick within the MyUPMC Patient Portal creates a method through which UPMC can report specific patient actions taken on the UPMC website and Patient Portal to Facebook for purposes of ad measurement and re-targeting.

235. Facebook instructs developers on how to set up their Google Campaign Manager to send automated regularly scheduled reports to Facebook:²⁰

²⁰ <https://www.facebook.com/business/help/565734646951134>

▼ **Set Up Recurring Report for Automated Mapping and Cost Data Import**

1. Go to **Google Campaign Manager**.
2. Select **Reporting & Attribution** from the dropdown menu.
3. Select **Report Builder**, then click **New Report** and select a standard report.
4. Enter a name for the report. For **File type**, select **CSV**. For **Date Range**, select **Yesterday**.
5. For **Filters**, select the accounts or campaigns where tags are currently installed.
6. For **Dimensions** and **Metrics**, select the following:
Date, Advertiser, Advertiser ID, Campaign, Campaign ID, Site (DCM), Site ID (DCM), Placement, Placement ID, Ad, Ad ID, Ad Type, Impressions, Clicks, Media Cost
7. Under **Schedule**, click to check the box next to **Active**. For **Repeats**, select **Daily**. For **Every**, select **1 day**. For **Starts**, select today's date. This report will run until it expires, so set **Expires** to a date as far into the future as possible.
8. For **Share with**, click **Add people** and paste the Facebook-provided **Mapping Import Email** and **Cost Import Email** addresses, as applicable. Click **Save**.



236. In the absence of formal discovery and access to UPMC’s Google and Facebook marketing accounts, it is impossible to know whether and how much data is disclosed to Facebook through this method. However, the fact that a Google DoubleClick ‘fbp’ cookie identifier is created and caused to be disclosed to Google when a patient sends communications inside the Patient Portal at UPMC strongly suggests that UPMC is, in fact, using this combined Google and Facebook functionality to make disclosures of patient data to Facebook of activity within the Patient Portal.

Adobe

237. Though best known for its ubiquitous PDF software, Adobe also has a data division that helps web developers and marketers sell targeted advertising.

238. UPMC deploys Adobe source code on pages relating to patient communications about specific medical providers and appointment requests.

239. The Adobe Audience Manager source code deployed by UPMC is a “data management platform” that helps developers and marketers “build unique audience profiles” to “identify your most valuable segments and use them across any digital channel.”²¹

240. UPMC also deploys Adobe source code that causes transmissions of data to the domain demdex.net. The Adobe source code causes the transmission of patient IP addresses and unique cookie values to Adobe connected to the contents of communications that UPMC exchanges with patients relating to specific medical providers and appointment requests.

241. The Adobe cookies used by UPMC are named demdex, dexptp, and dpm.

242. The demdex cookie is a Unique User ID that “helps Audience Manager perform basic functions such as visitor identification, ID synchronization, segmentation, modeling, reporting, etc.”²²

243. The dexptp cookie “record[s] the last time it made a data synchronization call” and “contains a data provider name or ID and a UNIX UTC timestamp.”²³

244. The DPM in the DPM cookie “is an abbreviation for Data Provider Match. It tells internal, Adobe systems that a call from Audience Manager or the ID service is passing in customer data for synchronization or requesting an ID.” In Audience Manager, a DPM call “sends data to the Data Collection Servers and Profile Cache Servers.”²⁴ In turn, the Data Collection Servers

²¹ <https://www.adobe.io/apis/experiencecloud/audiencemanager.html>

²² https://marketing.adobe.com/resources/help/en_US/whitepapers/cookies/cookies_am.html

²³ *Id.*

²⁴ https://marketing.adobe.com/resources/help/en_US/aam/demdex-calls.html

“create[] and manage[] device IDs and authenticated profile IDs. This includes identifiers such as data provider IDs, user IDs, declared IDs, integration codes, etc.”²⁵

245. Adobe discloses the different types of uses that developers make of its products:²⁶

What information is collected when a company uses Adobe Experience Cloud?

When a company uses Adobe Experience Cloud solutions, that company chooses how to use the solutions, including what information to collect and send to its Adobe Experience Cloud account. Examples of the types of information that may be collected include the following, depending on the particular Adobe Experience Cloud solution and the jurisdiction of the company:

- Where you go and what you do on that company's websites, apps, or social media pages
- Your web browsing activity, including the URLs of the company's web pages you visit
- The URL of the page that displayed the link that you clicked on, which brought you to that company's website
- The web search you performed that led you to that company's website
- Information about your web browser and device, such as device type, browser type, advertising identifier, operating system, connection speed, and display settings
- Your IP address (or partial IP address, depending on how the company has configured the solution), which may be used to approximate your general location
- Location information from your mobile device or web browser
- Social media profile information
- Information you may provide on that company's website, app, or when interacting with that company's social media pages, such as information you provide on registration forms
- Ad campaign success rates, such as whether you clicked on a company's ad and whether viewing or clicking on the ad led to your purchase of that company's product
- Items you've purchased or placed in your shopping cart on that company's website or app

246. Adobe further states that it requires developers to disclose their use of Adobe:

What privacy choices do you have about a company's use of Adobe's Experience Cloud solutions?


For more information about how a company uses Adobe's Experience Cloud solutions, please refer to that company's privacy policy. Adobe asks its business customers to provide privacy policies describing:

- Their privacy practices in connection with Adobe Experience Cloud
- How you can set your preferences for the collection or use of information obtained by the company in connection with Adobe Experience Cloud

247. UPMC does not disclose its use of Adobe to patients.

248. Like Google Analytics and Google DoubleClick, Adobe source code is capable of being used to make disclosures to Facebook.

249. Adobe instructs developers on how to integrate with the Facebook Pixel, and describes the benefits of such an integration:



Facebook Pixel
Adobe
Allows you to track conversions along with other events and send this data to Facebook.

²⁵ https://marketing.adobe.com/resources/help/en_US/aam/c_compcollect.html

²⁶ <https://www.adobe.com/privacy/experience-cloud.html>

250. UPMC deploys source code that causes the transmission of an ‘fbp’ cookie identifier to Adobe on patient communications pages about specific providers and appointment requests. Much like the integration of Google and Facebook explained above, in the absence of formal discovery and access to UPMC’s Adobe and Facebook marketing accounts, it is impossible to know whether and how much data is disclosed to Facebook through this method. However, the fact that an Adobe ‘fbp’ cookie identifier is created and caused to be disclosed to Adobe when a patient sends communications relating to specific providers and appointment requests, strongly suggests that UPMC is, in fact, using this combined Adobe and Facebook functionality.

Microsoft (Bing Ads)

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

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

253. UPMC deploys Microsoft source code on the UPMC homepage and pages relating to patient communications about specific medical providers, conditions, and appointment requests.

Salesforce (KruX Digital)


254. Salesforce is the world’s largest customer relations management software provider. In 2016, it acquired KruX Digital, a data-management platform, for \$700 million.

255. Salesforce claims that every month, through KruX (now Salesforce DMP), it interacts with “more than 3 billion browsers and devices, supports more than 200 billion data collection events, processes more than 5 billion CRM records, and orchestrates more than 200 billion personalized consumer experiences.”²⁷

²⁷ <https://www.salesforce.com/blog/2017/05/kruX-is-now-salesforce-dmp.html>

256. With that massive trove of data, Salesforce matches user profiles for its customers. It explains:²⁸

User Matching and Match Rates FAQ



Rainer Teschke
May 06, 2019 08:51

Follow

What is user matching?

Salesforce Audience Studio works with many partners in the advertising technology ecosystem. Salesforce Audience Studio can receive user-level data from partners (e.g. 3rd Party Data Providers) or we can send user-level data to partners (e.g. Activation Partners). Both Salesforce Audience Studio and partners use their own user ID to identify users. To know which Krux User ID (KUID) corresponds to a partner's user ID for the same person, we need to user match. Either Salesforce, the partner, or both, fire the other party's user match pixel when their own pixel fires on site for the user match to happen. This is how the other party is able to know which user ID is associated to the user currently on the page. Either, or both, of the parties create and store a "user match table" containing the matched user IDs of both parties.

257. Salesforce states that it has typical match rates of between 60 to 90 percent.

258. UPMC deploys Salesforce's matching technologies to identify patients. In particular, it engages in cookie synching for the value of a cookie called 'kuid.'

259. UPMC deploys Salesforce source code on its homepage and those relating to patient communications about specific medical providers, conditions, and appointment requests.

Crazy Egg

260. Crazy Egg is a service that developers use to improve website performance by recording user interactions on a website to create heatmaps, scroll maps, and recordings of user communications.

261. UPMC deploys Crazy Egg source code on all parts of the UPMC.com website

²⁸ <https://konsole.zendesk.com/hc/en-us/articles/115006072448-User-Matching-and-Match-Rates-FAQ>

other than the Patient Portal and the Patient Portal log-in page, including pages relating to patient communications about specific medical providers, conditions, and appointment requests.

262. UPMC's use of Crazy Egg source code causes data transmission to Crazy Egg via its domain, cloudfront.net, that includes patient IP addresses and the content of patient communications with UPMC.

LivePerson

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

264. LivePerson tracks consumers, including patients at the UPMC.com website, with IP addresses and cookie identifiers.

265. UPMC deploys Live Person source code on all parts of the UPMC.com website, including the Patient Portal, the Patient Portal log-in page, and pages relating to patient communications about specific medical providers, conditions, and appointment requests.

Kenshoo

266. Kenshoo claims to be “the leading technology platform for brands looking to plan, activate and amplify effective marketing across the most-engaging digital channels.” It states that it is “the only marketing solution that provides data-driven insights and optimization technology to help make informed decisions and scale performance across critical publishers” that include Facebook, Google, and Microsoft.²⁹

267. Kenshoo tracks consumers, including UPMC patients, using IP addresses and cookie identifiers.

²⁹ <https://kenshoo.com/company/>

268. UPMC deploys Kenshoo source code on the Patient Portal log-in page.

269. UPMC's deployment of Kenshoo source code is funneled through Google DoubleClick.

Decibel Insight

270. Decibel Insight claims to be able to “capture[] unique experience data, enriched by machine learning, to reveal digital body language, understand user state of mind and pinpoint problem areas of your website, web applications, and native apps.”³⁰

271. Decibel Insight tracks consumers, including UPMC patients, using IP addresses and cookie identifiers.

272. UPMC deploys Decibel Insight source code on pages relating to its patients' communications about specific medical providers and appointment requests.

FullStory

273. FullStory uses technology to help developers discover “when, where, and why [their] customers experience friction on [their] website or app.”³¹

274. FullStory tracks consumers, including UPMC patients, using IP addresses and cookie identifiers.

275. UPMC deploys FullStory source code on pages relating to patient communications about specific medical providers.

Verint Foresee

276. Verint Foresee is a division of Verint, which bills itself as a “customer

³⁰ <https://www.decibelinsight.com/about/>

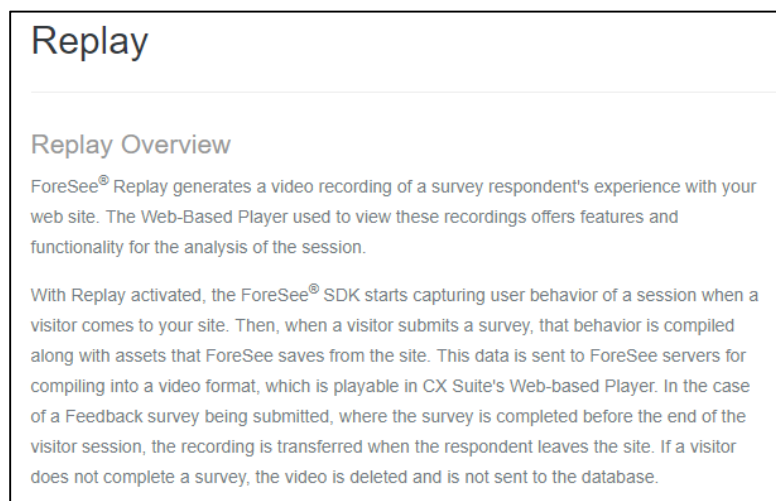
³¹ <https://www.fullstory.com/>

engagement company” that provides a customer engagement and cyber-intelligence platform with four parts: (1) data capture; (2) data processing; (3) data analysis and automation, including “identity extraction;” and (4) data visualization.³²

277. Foresee provides web developers with the “ForeSee CX Suite,” a solution to power customer experience intelligence.

278. UPMC deploys Foresee source code on all parts of the UPMC.com website other than the Patient Portal and the Patient Portal log-in page.

279. Among other items, Foresee provides a “Replay” service that it describes as follows:



280. Foresee instructs developers on “Replay Masking” to prevent “the capture of personally identifiable information.” Foresee’s instructions allegedly cause the masking to occur before the recording is transmitted to the Foresee server. Plaintiffs are without knowledge as to whether UPMC utilizes Foresee’s specific masking technology.

SiteImprove

281. SiteImprove is a company that helps developers improve their websites.

³² <https://www.verint.com/our-company/our-vision/>

282. SiteImprove informs developers that it “collects and processes personal data belonging to any individual appearing on customers’ websites on which the SiteImprove Intelligence Platform is used.” SiteImprove defines “personal data” as “any information that directly or indirectly identifies or is identifiable to you as a natural person. Personal data includes your name, address, email, telephone number, IP address, or any other identifier through which you may be contacted online or offline.”³³

283. UPMC deploys SiteImprove source code on all parts of the UPMC.com website except the Patient Portal and Patient Portal log-in page.

LiveRamp

284. LiveRamp provides a service called IdentityLink that it claims “is an identity resolution service that ties data back to real people and makes it possible to onboard that data for people-based marketing initiatives across digital channels.”³⁴



³³ SiteImprove, Privacy Policy, <https://siteimprove.com/en/privacy/privacy-policy/>

³⁴ <https://liveramp.com/discover-identitylink/>

285. UPMC deploys LiveRamp source code on pages relating patient search queries to “Find-A-Doctor.”

The Trade Desk

286. The Trade Desk is an online advertising company that “helps advertisers and their advertising agencies manage digital advertising campaigns across many channels, such as websites, apps, audio, smart tvs, and other video.”³⁵

287. The Trade Desk states that the data it collects is not anonymous, but instead claims it “is pseudonymous, which means that it does not directly identify people.”³⁶

288. The Trade Desk retains the information for “up to 18 months before [The Trade Desk] aggregate[s] it.” The “pseudonymous” data includes:

The data our Platform collects and processes:	<p>Pseudonymous data such as:</p> <ul style="list-style-type: none">• unique cookie and device identifiers• mobile device advertising identifiers• IP addresses• web browsing history from advertising impressions we see• interest information inferred by us from web browsing history• interest information stored and/or used on the Platform by clients and partners• location information• browser and device type, version and settings
--	---

289. As described by The Trade Desk, the “pseudonymous” data it collects is personally identifiable information under HIPAA.

290. UPMC deploys The Trade Desk source code on pages relating to patient search queries to “Find-A-Doctor.”

³⁵ <https://www.thetradedesk.com/general/privacy>

³⁶ *Id.*

UPMC Assures Patients That It Protects Their Personally Identifiable Information

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

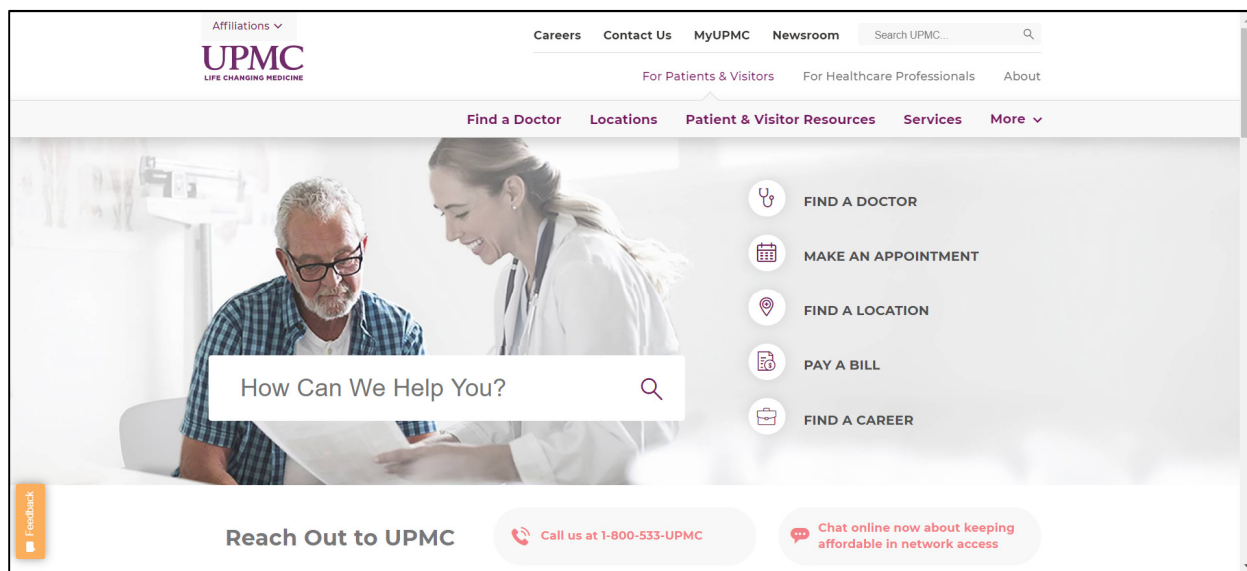
292. Patients who exchange communications with Defendant at UPMC.com and the UPMC Patient Portal have a reasonable expectation that their communications will remain confidential.

293. UPMC does not make any disclosure on its website that would sufficiently alert patients that it discloses, and causes to be transmitted to third parties, patients' personally identifiable data and communications.

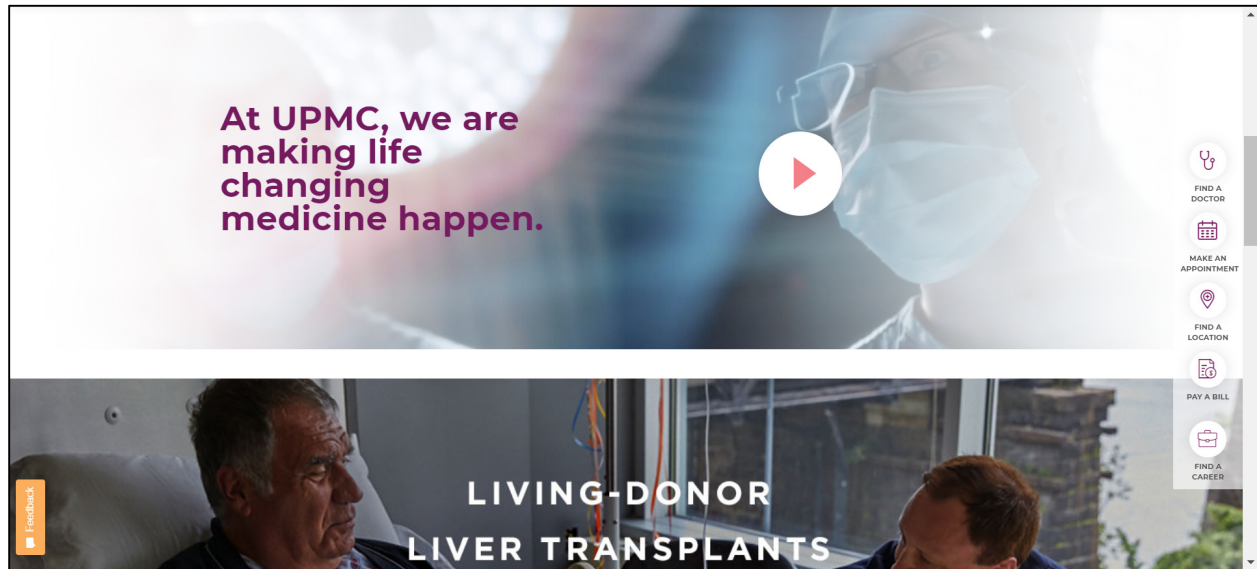
294. To the contrary, UPMC's various privacy statements reassure patients that their data is protected and confidential, and give patients the impression that its data practices at UPMC.com and myupmc.upmc.com are "completely anonymous."

295. The UPMC homepage contains a sub-footer with a link to "Privacy Information."

296. The link is inconspicuous and can only be viewed if a patient scrolls down through four full screens of content, as shown below.



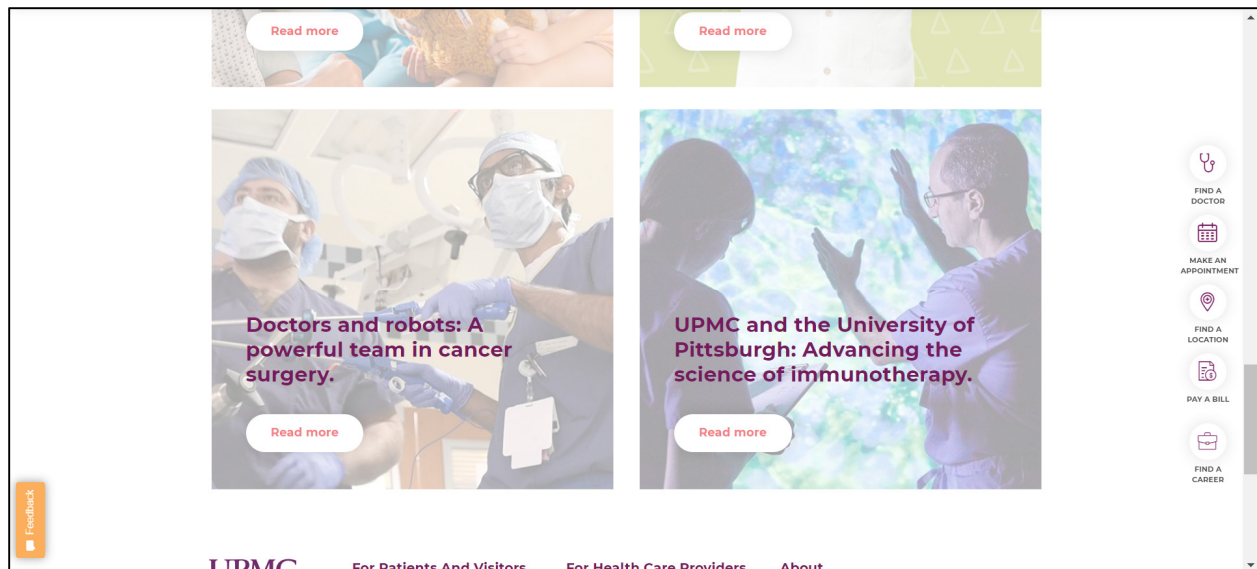
Homepage, Screenshot 1



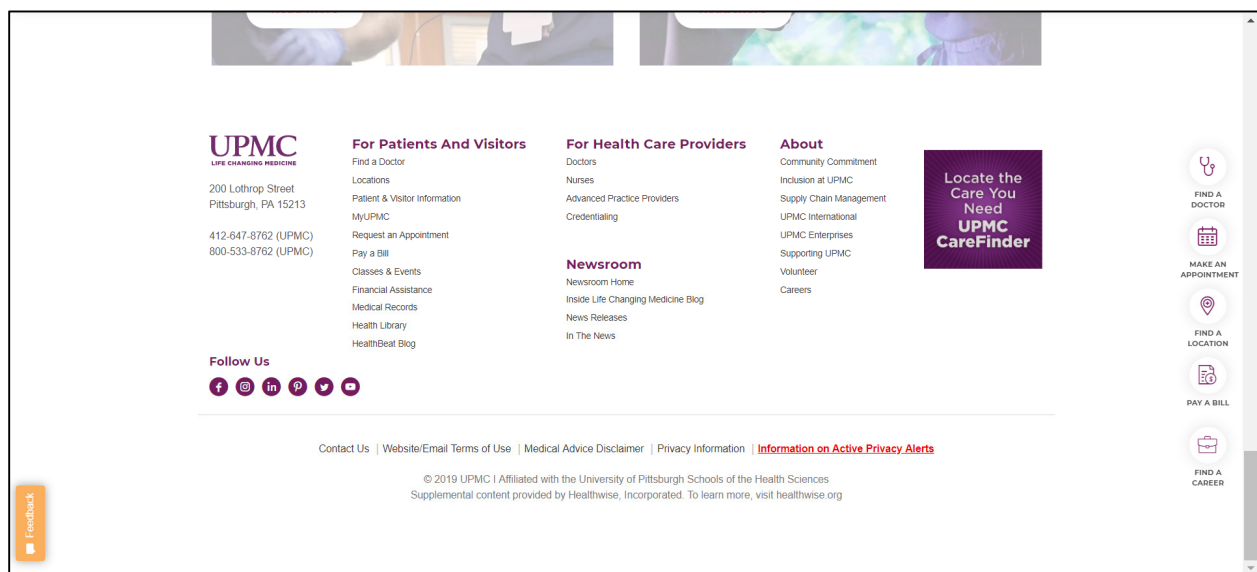
Homepage, Screenshot 2



Homepage, Screenshot 3



Homepage, Screenshot 4



Homepage, Screenshot 5

297. By clicking the “Privacy Information” link, a patient is taken to the following page:

The screenshot shows the UPMC website's 'Privacy Information' page for patients. The header includes the UPMC logo and navigation links. The main content area has a heading 'Privacy Information For Our Patients' and a list of links: [Privacy and Breach Alerts](#), [UPMC Notice of Privacy Practices](#), [UPMC EU Notice of Privacy Practices](#), [Organized Health Care Arrangements that UPMC Participates In](#), and [Consent for Treatment, Payment and Health Care Operations \(PDF\)](#). A sidebar on the left lists various patient resources.

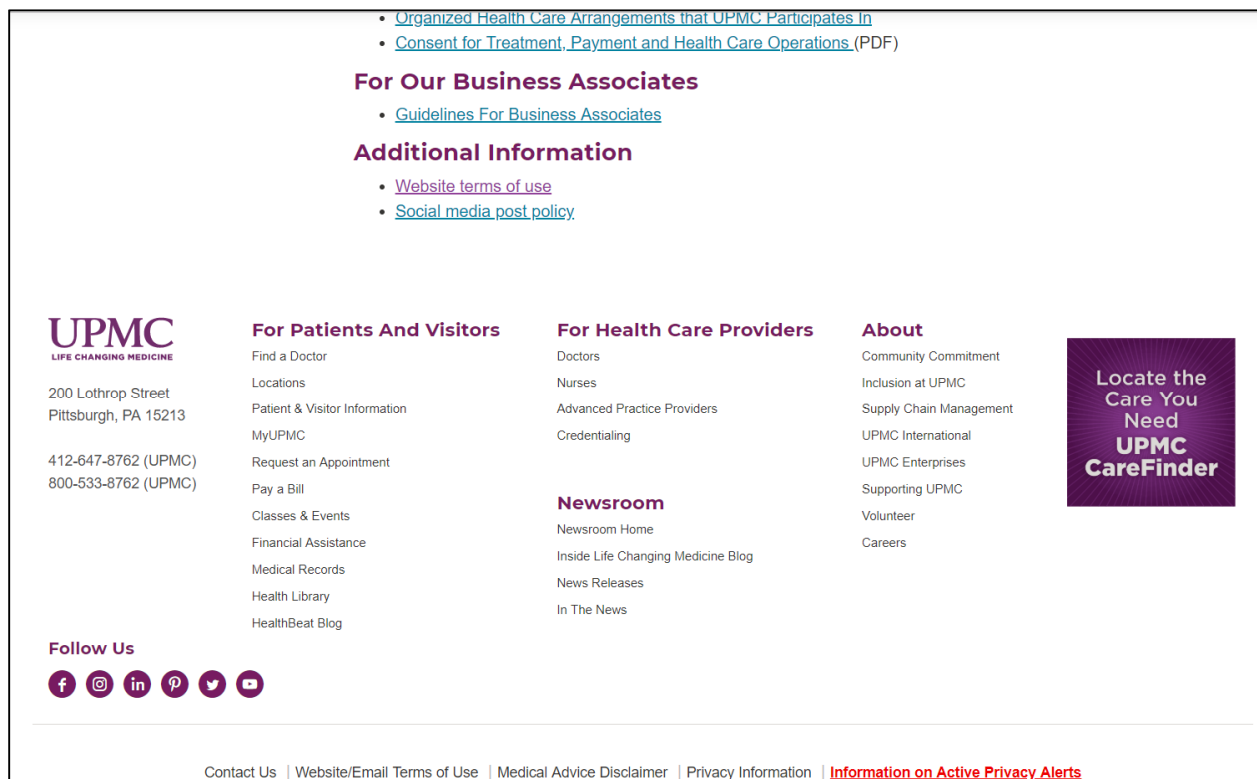
298. The first and most prominent promise “For Our Patients” is that “*UPMC is committed to keeping patient information confidential and secure.*”

299. The UPMC Notice of Privacy Practices applies to patients.

300. On the “UPMC Notice of Privacy Practices” page, UPMC states that it may share a patient’s health information for marketing purposes, but only when it “discuss[es] such products or services with you face to face or to provide you with an inexpensive promotional gift related to the product or service.” For all “other types of marketing activities,” UPMC promises to “obtain your written permission before using or sharing your health information.” It further expressly promises, “We will not sell your identifiable health information to others without authorization.”

10. **Marketing Activities.** We may use or share your health information for marketing purposes without your permission when we discuss such products or services with you face to face or to provide you with an inexpensive promotional gift related to the product or service. For example, you may receive samples of products or drugs during a visit to a UPMC hospital or facility. For other types of marketing activities, we will obtain your written permission before using or sharing your health information. We will not sell your identifiable health information to others without authorization.

301. If a patient scrolls further down on the “Privacy Information” page, he/she will see a link to “Website terms of use” under the heading, “Additional Information.”



302. The website “terms of use” link is not visible unless a patient scrolls past the link for “UPMC Notice of Privacy Practices.”

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

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

305. Browse-wrap statements do not enforceable contracts against consumers.

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

307. Consumer surveys consistently show that a majority of Americans falsely believe that the existence of a privacy policy means that “the company keeps confidential all the information it collects on users.”³⁷

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

309. On the purported “Website terms of use” page, until recently, Defendant stated that it uses advertising cookies for purposes of “retargeting and remarketing” but misleadingly stated that the data collected is “completely anonymous” and that “[n]one of this information, individually or grouped together, can be traced back to you.”

UPMC’s Admission to Disclosure of Patient Personal Information to Third Parties

310. At some point in the late summer or early fall of 2019, UPMC changed the language of its disclosures on its purported website privacy policy, removing the statements, “Data collected by UPMC for advertising or marketing purposes is completely anonymous, and only includes information such as the browser type, user location (municipality, not home or street address), IP address, date and time of visit, domain type, and your activity on the website. None of this information, individually or grouped together, can be traced back to you.”

311. However, rather than honestly disclose that its use of such tools causes disclosure

³⁷ Aaron Smith, Half of Americans Don’t Know What a Privacy Policy Is, Pew Research Center (Dec. 4, 2014) (Reporting that more than half of Americans falsely believe, “When a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users.”), available at <https://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/>.

of personally identifiable data about patients to third parties, UPMC now states, “We also may permit selected marketing partners to match and re-identify you, but only if you have voluntarily provided UPMC with your email address for the receipt of marketing and related information.”

312. In truth, UPMC sends personally identifiable information about patients and website visitors to third parties regardless of whether they have voluntarily provided UPMC with their email address for the receipt of marketing and related information.

313. UPMC’s new purported Privacy Policy now states, “UPMC does NOT collect or re-identify the following information in this process: Protected Health Information (PHI) ... Information or browsing behavior related to sensitive subjects, including but not limited to sexual health, cancer, substance abuse or disorders, and mental health ... or billing information.”

314. But UPMCs promise not to use such tools for PHI, “sensitive subjects” or billing information is false or deceptive. The third-party tracking tools deployed by UPMC continue to be deployed on the Patient Portal log-in page, inside the patient portal, and on pages relating to sensitive subjects.

315. When a patient signs up for the Patient Portal at myupmc.upmc.com, they are presented with a separate, purported Terms and Conditions sheet. Such terms and conditions are not enforceable against patients because UPMC purports to reserve for itself the right to change any of the terms at any time “at UPMC’s sole discretion.”

316. Regarding privacy, UPMC promises the following for the Patient Portal:

Privacy

UPMC is committed to safeguarding your personal information. As described in our Privacy Statement and Notice of Privacy Practices, we keep the personal information of our patients and members in the strictest confidence. UPMC complies with applicable laws, regulations, standards, and guidelines established by governmental agencies and accepted accrediting organizations at all times. These include the European Union's General Data Protection Regulation, where applicable. If you have any questions concerning the confidentiality of your personal information that has been entrusted to UPMC, please contact UPMC's Office of Patient and Consumer Privacy at 412-647-5757, or 1-800-533-UPMC (8762).

Detailed privacy information (including the HIPAA Notice of Privacy Practices) can be found at:

UPMC: <http://www.upmc.com/patients-visitors/privacy-info/Pages/default.aspx>

UPMC Health Plan: <https://www.upmchealthplan.com/privacy.aspx>

317. Despite these assurances of confidentiality, UPMC routinely discloses and causes personally identifiable patient data and communications to be transmitted to third parties without patient knowledge, consent, authorization, or any further action of the patient.

UPMC's False and Misleading Statements in Its Notice of Privacy Practices

318. Federal law requires UPMC to (a) provide patients with a hard copy of its HIPAA Notice of Privacy Practices, and (b) post the notice at both its physical and web properties.

319. The UPMC "Notice of Privacy Practices" is available via UPMC.com as a webpage at <https://www.upmc.com/patients-visitors/privacy-info/notice-of-privacy-practice#fullnotice> and via a link to a PDF: <https://www.upmc.com/-/media/upmc/patients-visitors/privacy-info/documents/hippa-nopp.pdf>.

320. The UPMC Notice of Privacy Practices webpage is attached as Exhibit 1.

321. The UPMC Notice of Privacy Practices PDF is attached as Exhibit 2.

322. The UPMC Notice of Privacy Practices applies to all patients.

323. The UPMC Notice of Privacy Practices does not distinguish between patient data collected in person, by telephone, or by electronic communication.

324. The UPMC Notice of Privacy Practices includes numerous false or misleading statements regarding patient privacy.

325. The UPMC Notice of Privacy Practices webpage starts with a summary and the following promise, “At UPMC, we are committed to protecting the privacy of your medical information, as federal and state laws require. When we say “information,” we mean health, treatment, and payment information that identifies you.” This statement is false and misleading because UPMC routinely discloses information about patients to Facebook, Google, and others that identify the patients and provide information about patient health, treatment, and payment information.

326. The UPMC Notice of Privacy Practices webpage further promises, “All people and places that make up UPMC must follow the Notice.” This statement is false and misleading because UPMC routinely discloses identifiable information about patients to Facebook, Google and others at its web properties. As a result, the web property and persons at UPMC who design and run the web property do not follow the notice.

327. The UPMC Notice of Privacy Practices PDF does not include a summary. After the summary section, Exhibit 1 and Exhibit 2 contain identical text.

328. The UPMC Notice of Privacy Practices then states, “UPMC may share and use your health information for purposes of treating you, obtaining payment for services provided to you, health care operations as described in this Notice, as well as purposes authorized by you or permitted by law.” This statement is false and misleading because it omits that UPMC also shares with third parties and uses health information for marketing purposes that are not for purposes of treatment, payment, health care operations, or authorized by the patient.

329. Under the bold heading, “Our Duty to Protect Your Health Information,” UPMC promises, “We are required by law to: [m]ake sure that information that identifies you is kept private and is used in accordance with this notice.” This promise is false and misleading because

UPMC routinely shares information that identifies patients with third parties, including Facebook, Google, and many others.

330. The UPMC Notice of Privacy Practices then discloses 14 situations in which it shares personally identifiable patient information with others. This statement is false and misleading because it omits to inform its patients that Defendant routinely discloses personally identifiable patient data to Facebook, Google, and many others for purposes that are not stated.

331. The UPMC Notice of Privacy Practices discloses it may use or share patient information for marketing purposes in limited situations:

Marketing Activities. We may use or share your health information for marketing purposes without your permission when we discuss products or services with you face to face or to provide you with an inexpensive promotional gift related to the product or service. For example, you may receive samples of products or drugs during a visit to a UPMC hospital or facility. For other types of marketing activities, we will obtain your written permission before using or sharing your health information. We will not sell your identifiable health information to others without authorization.

This promise is false and misleading because the types of marketing activities at issue in this matter are not covered by the disclosure and UPMC does not obtain patients' written authorization to share their health information with Facebook, Google, or the other third parties identified herein. It is also false and misleading because UPMC sells the identifiable health information to others without authorization. The UPMC sale occurs in a barter exchange whereby UPMC shares the data with the third parties in exchange for enhanced marketing services.

332. The UPMC Notice of Privacy Practices then promises:

Except as stated in Sections A and B, your written permission is required before we can use or share your health information with anyone outside of UPMC. This permission is provided through a form. If you give us permission to use or share health information about you, you may cancel the permission, in writing, at any time. If you cancel your permission, we will no longer use or share your health information for the reasons you have given us in your written permission. However,

we are unable to take back any information that we have already shared with your permission.

This statement is false and misleading because UPMC did not obtain written permission for patients “through a form” to use or share patient information with Facebook, Google, or any of the other third parties identified herein.

333. The UPMC Notice of Privacy Practices then promises, “In the event that a breach of your protected health information occurs by UPMC or one of its Business Associates, you will be provided with written notification as required by law.” This statement is false and misleading because UPMC has not provided written notification to patients that it routinely discloses their protected health information to third parties for marketing purposes without their authorization.

334. UPMC’s Notice of Privacy Practices is required by federal law to be provided to patients in hard copy form and to be posted at UPMC properties. To the extent there is any conflict in terms between the Notice of Privacy Practices and other privacy statements by UPMC, the Notice of Privacy Practices governs first.

UPMC’s False and Misleading Statements in the MyUPMC Terms of Use

335. UPMC’s purported MyUPMC Terms of Use is placed on the website and available to be viewed by patients during the sign-up process for UPMC.

336. The purported MyUPMC Terms of Use is attached as Exhibit 3.

337. In a heading under “Privacy,” UPMC promises, “***UPMC is committed to safeguarding your personal information.***” (Emphasis added.) This statement is false and misleading because UPMC routinely discloses patient personal information to third parties, including Facebook and Google, for marketing purposes and without patients’ authorization.

338. UPMC next promises, “As described in our Privacy Statement and Notice of

Privacy Practices, we keep the personal information of our patients and members in the strictest confidence.” This statement is false and misleading because UPMC does not keep the personal information of patients and members in strictest confidence, but instead routinely discloses patient personal information to third parties for marketing purposes and without patients’ authorization.

339. UPMC next promises, “UPMC complies with applicable laws, regulations, standards, and guidelines established by governmental agencies and accepted accrediting organizations at all times.” This is false and misleading because UPMC fails to comply with several laws, regulations, standards, and guidelines, as alleged herein.

340. Under the heading, “Collection and Use of Identifiable Information,” UPMC next promises, “We may ask you to provide us with identifiable personal information while using our websites and apps. This information is collected and used only for the purposes indicated where and when the information is requested or collected. If we wish to use your personal information for a new or different purpose, we will offer you the means to consent to this purpose at the point where the use of your personal information is requested. *Except as requested by you, or as indicated on the webpage or app where your information is requested, we do not disclose identifiable personal information to other organizations.*” (Emphasis added.) This statement is false and misleading because UPMC routinely discloses identifiable personal information about patients to other organizations, including Facebook and Google without patient authorization.

341. UPMC discloses, “As you browse UPMC.com, advertising cookies will be placed on your computer so that we can understand what you are interested in. Our advertising and marketing partners then enable us to present you with advertising on other sites, or with marketing information, based on your previous interaction with UPMC.com.” This is false and misleading because it only discloses that UPMC is able to track and understand patient interests and omits that

the advertising cookies are third-party cookies used by those third parties to create detailed profiles of individual patients with their medical information, and to be used for purposes beyond UPMC or the patient's care. Plaintiffs here do not complain of UPMC's first-party tracking. As patients, Plaintiffs expect that UPMC maintains records of their communications, and, in fact, UPMC has access to Plaintiffs' entire medical records.

342. UPMC next states, "These advertising partners, as members of the Network Advertising Initiative ("NAI") may have their own privacy policies as well. To remove yourself from some or all NAI member advertising programs, please visit the NAI Opt-Out Page and follow the relevant instructions. Please note that if you delete, block, or otherwise restrict cookies on your computer, or if you use a different computer or Internet browser, you may need to renew your NAI opt-out choice." These statements are false and misleading because:

- a. A substantial percentage of the third parties to whom UPMC makes disclosures for marketing purposes are not members of the NAI. The unauthorized non-NAI third-party recipients of UPMC patient data include Facebook, LivePerson, Verint Foresee, Crazy Egg, Decibel Insight, and Sales Force.
- b. Google Analytics does not use cookies for identification purposes.
- c. UPMC has not disclosed the presence of any third-party trackers anywhere in this or any other purported privacy policy; and
- d. The opt-out instructions provided by UPMC do not block tracking.

343. The NAI opt-out does not block tracking from third parties; instead, it ensures that tracking will continue, and only purportedly blocks advertisements from some third parties from being based on a user's web-browser communications.

344. UPMC next promises, "Data collected *by UPMC* for advertising or marketing

purposes includes information such as the browser type, user location (municipality, not home or street address), IP address, date and time of visit, domain type, and your activity on our website.”

This statement is false and misleading because it omits that UPMC discloses the same data about patients with third parties, including Facebook, Google, and others for whom such data is personally identifiable. Plaintiffs here do not complain of UPMC’s first-party tracking. As patients, Plaintiffs expect that UPMC maintains records of their communications, and, in fact, UPMC has access to Plaintiffs’ entire medical records.

345. UPMC next promises, “We also may permit selected marketing partners to match and re-identify you, but only if you have voluntarily provided UPMC with your email address for the receipt of marketing and related information.” UPMC defines “re-identification” as “a process by which anonymized data is matched with personally identifiable information.” These statements are false and misleading because:

- a. The Facebook Pixel works by matching users with their Facebook accounts;
- b. The data disclosed by UPMC to third parties is not anonymous, but instead is identifiable by nature; and
- c. UPMC discloses the non-anonymous data to third parties regardless of whether a patient has “voluntarily provided” UPMC with their “email address for the receipt of marketing and related information.”

346. UPMC next defines “personal data or personal information” as “any information about an individual used to identify that person.” As described herein, that includes the data elements that UPMC routinely discloses to third parties for marketing purposes in the absence of patient authorization, including Internet cookies, IP addresses, and browser-fingerprint information.

347. UPMC next promises, “UPMC does not collect or re-identify the following information in this process: Protected Health Information (PHI), such as demographic information, medical histories, test and laboratory results, mental health conditions, and insurance information ... [i]nformation or browsing behavior related to sensitive subjects, including but not limited to sexual health, cancer, substance abuse or disorders, and mental health.” These statements are false and misleading because Defendant:

- a. routinely disclose patient protected health information, including data identifying a patient’s status as a patient and his/her medical communications at UPMC.com and myupmc.upmc.com; and
- b. routinely discloses information and browsing behavior relating to the sensitive subjects listed, including sexual health, cancer, substance abuse, mental health, and other conditions and treatments.

348. Under the heading, “How UPMC Protects Your Information,” UPMC promises, “UPMC maintains reasonable standards of security and confidentiality consistent with customary business practices to protect the information under our control from loss, misuse, and alteration.” This statement is false and misleading because UPMC routinely discloses patient personal information under its control to third parties for marketing purposes in the absence of patient authorization.

349. UPMC next promises, “We also limit access to our website and services by our own employees to the individuals we authorize for the proper handling of such information. Any employee found violating our standards of security and confidentiality will be subject to our disciplinary process. We require that our advertising and marketing partners follow the same policy for their internal staffs.” This statement is false and misleading because UPMC routinely

discloses patient personal information to third parties and does not require its advertising or marketing partners to protect the confidentiality of data disclosed by UPMC to ensure that it is not used for any other purpose.

350. UPMC informs users they can opt out of cookies through “browser settings and other tools.” But then UPMC states, “To the extent that a UPMC application requires cookies, restricting cookies may affect ability to use UPMC websites and apps. For example, MyUPMC requires that cookies be enabled on your browser for the website to work as designed. If you choose to block or restrict cookies on your computer, you will not be able to access all the functions and services available through MyUPMC.” These statements are false and misleading because:

- a. UPMC failed to disclose anywhere that it facilitates the placement, use, and disclosure of third-party cookies at UPMC.com and myupmc.upmc.com;
- b. Plaintiffs do not complaint about UPMC’s use of first-party cookies; and
- c. Without ever actually disclosing that it facilitates third-party use of cookies at its patient portal and web property, UPMC purports to condition a patient’s access to their medical records through MyUPMC on acceptance of third-party tracking, but then never informs patients of the difference between MyUPMC’s first-party cookies and third-party cookies.

351. Under the heading “Online Forms,” UPMC promises, “At times, UPMC may ask you for personal information while you are visiting our website. We ask for this information only to deliver materials that you have requested, to respond to a question you have asked, or to provide you with a product or service. When you enter data into an online form on our website, the personal information you type is protected and securely transmitted to us through a method such as Secure Sockets Layer (SSL). SSL is the standard method that websites use to protect visitors’ information

by coding or encrypting everything from credit card transactions to enrollment data.” This statement is false or misleading because, even if UPMC uses SSL encryption for every form communication, it also routinely discloses personally identifiable patient information associated with each form communication such that the equivalent information is shared with the third parties outside of the SSL method.

352. UPMC disclaims any responsibility for “links to other sites” from its web property. However, this case is not about any such “links to other sites.” Here, Plaintiffs complain about invisible web pixels through which UPMC discloses personally identifiable patient information.

353. UPMC next promises, “We will provide a secure transmission method for you to send us your personal information. While such secure transmission methods provide reasonable protections against unauthorized access, if you have concerns regarding the transmission of sensitive information, you should consider using nonelectronic communication methods.” This statement is false and misleading because *UPMC’s web property is designed to routinely re-direct and transmit personally identifiable patient information and the content of their communications to unauthorized third parties.*

354. UPMC next promises, “All UPMC staff and consultants who have access to or are involved with the processing of personal information have been trained to respect the confidentiality of your personal information.” This statement is false and misleading because UPMC routinely discloses patient personal information to third parties without patient authorization.

355. Finally, UPMC’s purported MyUPMC Terms of Use contains an unconscionable

and unenforceable Limitation of Liability clause that purports to waive all claims for damages resulting from a series of types of claims that, even if the clause were enforceable, does not include claims for UPMC's unauthorized disclosure and use of patient personal information and the contents of patient communications as alleged in any cause of action described herein.

UPMC's False and Misleading Statements in the Purported Website Privacy Statement

356. The UPMC Website Privacy Statement is included within UPMC's purported Website Terms of Use, which are unenforceable against patients because it is only provided via browser-wrap links that are not viewable on any page unless the user scrolls to the very bottom of the page through a submerged screen. Even after a user arrives on the Website Terms of Use page, the purported Website Privacy Statement is not viewable unless a user scrolls to a submerged screen.

357. UPMC's purported Website Privacy Statement creates additional reasonable expectations of privacy.

358. The initial overview appears as such:

Website Privacy Statement

- Modern information and communication technologies play a fundamental role in the activities of an organization like UPMC. We are based in the United States of America. Our principal activity is the delivery of health care services.
- Our Privacy Statement covers the UPMC, its subsidiaries and any of its websites accessible via the primary websites listed below:

Organization Name: UPMC

Address: 200 Lothrop St.

City, Zip: Pittsburgh, 15213

State: PA

Country: USA

Primary websites: www.upmc.com; www.chp.edu; hillman.upmc.com; www.altoonaregional.org

- You can access our website home page and browse our site without disclosing your personal data.
- We collect the personal information that you may volunteer while using our services.
- We do not collect information about our visitors from sources outside of UPMC, such as public records or bodies, or private organizations.
- We do not collect or use personal data for any purpose other than that indicated on the Web pages where the information is requested or collected.
- If we wish to use your personal information for a new purpose, we offer you the means to consent to this new purpose by indicating in a box at the point on the site where personal data is collected.
- Except as requested by you or indicated on the Web page where your information is requested, we do not disclose your personal information to other organizations.

359. This overview contains several false and misleading statements.

360. UPMC starts its purported Website Privacy Statement with the promise, “You can access our website home page and browse our site without disclosing your personal data.” This is false and misleading because UPMC deploys third-party source code that routinely and automatically causes disclosure of patient personal data to third parties for marketing purposes and without patient authorization.

361. UPMC next promises, “We do not collect information about our visitors from sources outside of UPMC, such as public records or bodies, or private organization.” This is false and misleading because the third-party source code deployed by UPMC involves the sharing of data between UPMC and numerous private third-party organizations.

362. UPMC next promises, “We do not collect or use personal data for any purpose other

than that indicated on the Web pages where the information is requested or collected.” This is false or misleading because UPMC routinely uses patient personal data that it discloses to third parties for marketing purposes in the absence of patient authorization.

363. UPMC next promises, “If we wish to use your personal information for a new purpose, we offer you the means to consent to this new purpose by indicating in a box at the point on the site where personal data is collected.” This is false and misleading because UPMC discloses patient personal information to third parties for marketing purposes on every page of the website, regardless of whether a box is present on the page and without obtaining patient authorization or consent in any form.

364. UPMC next promises, “Except as requested by you or indicated on the Web page where your information is requested, we do not disclose your personal information to other organizations.” This is false or misleading because UPMC routinely discloses patient personal information to third-party organizations for marketing purposes without patient authorization.

365. UPMC then repeats the false and misleading statements and promises set forth in the MyUPMC policy as described above.

PLAINTIFFS’ EXPERT REPORT

366. Plaintiffs retained a computer expert named Richard Smith (“Smith”) to examine the operations of the UPMC and MyUPMC web-properties. Smith provided a report which is attached as Exhibit 4 to this Complaint.

CLASS ACTION ALLEGATIONS

367. Plaintiffs bring this class action and seeks certification of the claims on behalf of the following class (the “Class”):

All Pennsylvania residents who are, or were, patients of UPMC or any of its affiliates, and who used UPMC’s web properties, including, but not limited to, UPMC.com and the Patient Portal at myupmc.upmc.com.

368. Plaintiffs reserve the right to redefine the Class prior to certification.

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

370. The Class for whose benefit this action is brought is so numerous that joinder of all Class members is impracticable.

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

372. Plaintiffs are committed to prosecuting this action and have retained competent counsel experienced in litigation of this nature. Plaintiffs’ claims are typical of the claims of other Class members and Plaintiffs have the same interests as other Class members. Plaintiffs have no interests antagonistic to or in conflict with the interests of the other members of the Class. Plaintiffs are adequate representatives of the Class and will fairly and adequately protect the interests of the Class.

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

374. The expense and burden of individual litigation make it impracticable for members

of the Class to redress the wrongs done to them individually. If a class action is not permitted, Class members will continue to suffer losses and Defendant's misconduct will continue without proper remedy.

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

376. Plaintiffs anticipate no unusual difficulties in the management of this litigation as a class action.

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

378. There are questions of law and fact common to Class members that predominate over any questions affecting only individual members of the Class. A class action will generate common answers to the below questions, which are apt to drive resolution:

- a. Whether Defendant's practices relating to its disclosures of the Class communications with Defendant to third-party companies attached to personal information was intentional;
- b. Whether Defendant's practices relating to its disclosures of the Class communications with Defendant to third-party companies attached to personally identifiable information constituted a breach of provider-patient confidentiality;
- c. Whether Defendant's practices relating to its disclosures of Class communications with Defendant to third-party companies attached to personally identifiable information was a violation of the Pennsylvania "Wiretapping and Electronic Surveillance Control Act," 18 Pa.C.S.A. § 5725;
- d. Whether Defendant's practices amounted to an unfair business practice;
- e. Whether Defendant's practices violated Pennsylvania's identity theft laws;
- f. Whether Defendant's practices constituted negligent maintenance of the patient's personally identifiable data and communications;

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

COUNT I – BREACH OF PROVIDER-PATIENT CONFIDENTIALITY

379. Plaintiffs incorporate all prior paragraphs as if fully stated herein.

380. In Pennsylvania, medical providers have an obligation to their patients to keep communications, diagnosis, and treatment completely confidential.

381. Patients are aware of the promises of discretion contained in the Hippocratic Oath and must be able to rely on those promises.

382. Disclosure of confidential medical information by a medical provider in Pennsylvania without consent results in civil liability.

383. Plaintiffs are patients of Defendant.

384. Plaintiffs had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged at UPMC.com, on the log-in page for the UPMC Patient Portal, and within the MyUPMC patient portal.

385. Plaintiffs' reasonable expectations of privacy in the communications exchanged with Defendant were further supported by, but not limited to:

- a. Defendant's express statement, "UPMC is committed to safeguarding your personal information;"

- b. Defendant's express statement, "We keep the personal information of our patients and members in the strictest confidence;"
- c. Defendant's express statements on its website that its HIPAA Privacy Policy applied to its patients; and
- d. The other false and misleading statements set forth herein.

386. Contrary to its obligations as a provider and its express promises of confidentiality, UPMC deployed source code to disclose and transmit Plaintiffs' personally identifiable data and the contents of their communications exchanged with UPMC to numerous third parties.

387. The third-party recipients to whom Defendant disclosed Plaintiffs' personally identifiable data and communications include Google, Facebook, Adobe, Microsoft, Salesforce, CrazyEgg, LivePerson, Kenshoo, Decibel Insight, FullStory, Verint Foresee, SiteImprove, LiveRamp, and theTradeDesk.

388. Defendant's disclosures of Plaintiffs' personally identifiable information and the contents of their communications with UPMC were made without their knowledge, consent, authorization, or any further action on their part.

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

390. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable information and communications, Plaintiffs and Class members were damaged by Defendant's breach in that:

- a. Sensitive and confidential information that Plaintiffs and 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 from Plaintiffs and Class members and derived benefit therefrom without Plaintiffs' and Class members' knowledge or informed consent and without sharing the benefit of such value;
- d. Plaintiffs and Class members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- e. Defendant's actions diminished the value of Plaintiffs' and Class members' personal information; and
- f. Defendant's actions violated the property rights Plaintiffs and Class members have in their personally identifiable medical information and the content of their communications.

COUNT II - VIOLATION OF PENNSYLVANIA WIRETAPPING AND ELECTRONIC SURVEILLANCE CONTROL ACT

391. Plaintiffs incorporate all prior paragraphs as if fully stated herein.

392. The Pennsylvania "Wiretapping and Electronic Surveillance Control Act," 18 Pa.C.S.A. § 5701, *et seq.* (the "Act"), prohibits the intentional interception or the procurement of any other person to intercept any electronic communication in Pennsylvania without the consent of all parties to the communication, and the intentional use of the contents of any electronic communication, knowing or having reason to know, that the information was obtained through the interception of an electronic communication.

393. 18 Pa.C.S.A. § 5725 creates a civil cause of action for "[a]ny person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of this chapter [...] against any person who intercepts, discloses or uses or procures another person to intercept, disclose or use, such communication." 18 Pa.C.S.A. § 5725(a).

394. Pursuant to 18 Pa.C.S.A. § 5702, "electronic communication" refers to "[a]ny 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 photo-optical system,

except: (1) Deleted; (2) Any wire or oral communication; (3) Any communication made through a tone-only paging device; (4) Any communication from a tracking device.”

395. The Act protects both the sending and the receipt of electronic communications.

396. All communications described herein between Plaintiffs and UPMC qualify as electronic communications under Pennsylvania law because each are made using personal computing devices, including smartphones, that send and receive communications, in whole or in part, through the use of facilities used for the transmission of communications aided by wire, cable, or other like connections.

397. Pursuant to 18 Pa.C.S.A. § 5702, “intercept” means the “acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device,” with certain exceptions for law enforcement.

398. Pursuant to 18 Pa.C.S.A. § 5702, “contents” is defined as “any information concerning the substance, purport, or meaning of that communication.”

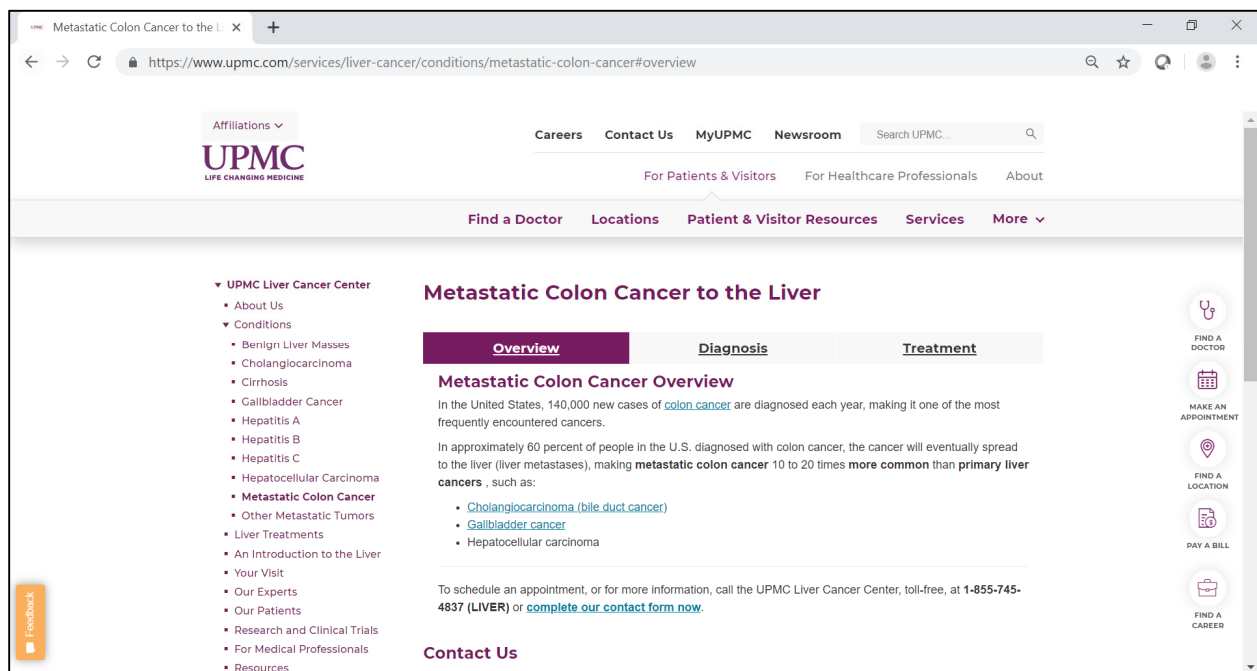
399. Together, the definition of “intercept” and “contents” prohibit the unauthorized acquisition of any information concerning the substance purport of meaning of a communication through the use of any electronic, mechanical, or other device.

400. Defendant violated the Act by procuring third parties, including Google, Facebook, Adobe, Microsoft, Salesforce and others, to acquire the content of electronic communications exchanged between Plaintiffs and Defendant without the consent of Plaintiffs.

401. The “content” that Defendant procured the third parties to acquire included the precise communications exchanged between Plaintiffs and Class members and the Defendant, in the form of GET requests, POST requests, and other requests and queries relating to specific medical providers, conditions, treatments, billings, and patient status.

402. For example, for the “Metastatic Colon Cancer” communication exchange, the content at issue includes “services/liver-cancer/conditions/metastatic-colon-cancer.”

403. The phrase “services/liver-cancer/conditions/metastatic-colon-cancer” is the precise content of a patient’s GET request communication sent to UPMC, and it is Pennsylvania Wiretap and Electronic Surveillance Act “content” of UPMC’s return communication to the patient because it “relates to the substance, purport, or meaning” of that return communication:



404. Defendant further violated the Act by knowingly using the intercepted communications for purposes of targeted advertising through processes known as re-targeting and re-marketing.

405. The third parties acquired the content of Plaintiffs’ and other patient Class members’ communications exchanged with Defendant contemporaneous to the electronic communications exchanged between Plaintiffs and Class members and Defendant.

406. By design, Defendant procured the third parties to acquire the content of the

Plaintiffs' communications while the communication between Defendant and Plaintiffs was still ongoing.

407. The third parties acquired the content of Plaintiffs' and other Class members' communications exchanged with Defendant through its deployment of source code that caused the content of such communications to be re-directed to the third parties.

408. Defendant's procurement of third parties to secretly acquire and record the content of Plaintiffs' and patient Class members' electronic communications was done without the Plaintiffs' or patient Class members' knowledge, consent, authorization, or any further action on their part.

409. As patients of Defendant, Plaintiffs and Class members have reasonable expectations of privacy that their personally identifiable data and communications with Defendant will not be disclosed by Defendant to third parties without their authorization.

410. Defendant further promised Plaintiffs and Class members that, as patients, their information was protected by HIPAA – which requires express and separate authorization to use a patient's personally identifiable information for marketing purposes unless the marketing involves face-to-face communications or small gifts of a nominal value.

411. Defendant further promised Plaintiffs and Class members that "UPMC is committed to safeguarding your medical privacy" and that it "keep[s] the personal information of [its] patients and members in the strictest confidence."

412. Defendant further promised Plaintiffs and non-patient Class members users of the UPMC website that Defendant deployed marketing technologies at UPMC.com, but that such technologies were "completely anonymous" and that "[n]one of this information, individually or grouped together, can be traced back to you."

413. By deploying the source code of the various third parties described above, Defendant knowingly procured those third parties to acquire and record personally identifiable patient data and communications.

414. Pursuant to 18 Pa.C.S.A. § 5725, any individual whose wire and/or electronic communication is unlawfully intercepted is entitled to recover (1) actual damages, but not less than liquidated damages computed at the rate of \$100 a day for each day of violation, or \$1,000, whichever is higher; (2) punitive damages; and (3) a reasonable attorney's fee and other litigation costs reasonably incurred. 18 Pa.C.S.A. § 5725(a)(1)–(3).

415. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable information and communications, Plaintiffs and Class members were damaged by Defendant's breach in that:

- a. Sensitive and confidential information that Plaintiffs and Class members intended to remain private is no more;
- b. Defendant eroded the essential confidential nature of the provider-patient relationship;
- c. Defendant took something of value from Plaintiffs and Class members and derived benefit therefrom without Plaintiffs and Class members knowledge or informed consent and without sharing the benefit of such value;
- d. Plaintiffs and Class members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- e. Defendant's actions diminished the value of Plaintiffs' and Class members' personal information; and
- f. Defendant's actions violated the property rights Plaintiffs and Class member patients have in their personally identifiable medical information and the content of their communications.

COUNT III – PENNSYLVANIA UNFAIR TRADE AND BUSINESS PRACTICES ACT

416. Plaintiffs incorporate all prior paragraphs as if fully stated herein.

417. The Pennsylvania Unfair Trade and Business Practices Act provides that “any person who purchases ... services primarily for personal, family, or household purposes and thereby suffers any ascertainable loss of money or property, real or personal, as a result of the use or employment by any person of a method, act, or practice declared unlawful by section 3 of this act, may bring a private action to recover actual damages or one hundred dollars, whichever is greater.” 73 P.S. § 201-9.2.

418. Plaintiffs and Class members are patients of Defendant who purchased health care services for personal, family, or household use.

419. Defendant’s acts described herein violated the Pennsylvania Unfair Trade and Business Practices Act in that Defendant’s acts and statements:

- a. Represented that the services had characteristics that they did not have; namely, that the health care services and communications with patients were treated by UPMC the same as HIPAA data; that UPMC is committed to safeguarding patient personal information; that UPMC “keep[s] the personal information of [its] patients and members in the strictest confidence;” that UPMC’s use of re-targeting and re-marketing technologies were “completely anonymous;” that “none” of the advertising and marketing tracking that UPMC conducted and procured others to conduct on its website could be traced back to a patient; and by the other false and misleading promises set forth above;
- b. Constituted fraudulent and deceptive conduct creating a likelihood of confusion or of misunderstanding for consumers, namely that Defendant’s actions fraudulently and deceptively created a likelihood of

confusion or misunderstanding on the part of patients who believed that their personally identifiable data and communications would not be disclosed by Defendant (their health care provider) to third parties without their authorization; and

- c. Involved knowingly false or misleading statements in UPMC's various privacy statements, including the enforceable its Notice of Privacy Practices that is required, by federal law, to be provided to patients; the purported MyUPMC Terms of Use, and the purported Website Terms of Use (provided in an unenforceable browsewrap statement).

420. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable information and communications and breach of its duties of confidentiality and specific privacy promises, Plaintiffs and Class members suffered an ascertainable loss of money or property in that:

- a. Sensitive and confidential information that Plaintiffs and Class members intended to remain private is no more;
- b. Defendant eroded the essential confidential nature of the provider-patient relationship;
- c. Defendant took something of value from Plaintiffs and Class members and derived benefit therefrom without Plaintiffs' and Class members' knowledge or informed consent and without sharing the benefit of such value;
- d. Plaintiffs did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- e. Defendant's actions diminished the value of Plaintiffs' and Class members' personal information; and
- f. Defendant's actions violated the property rights Plaintiffs and patients have in their personally identifiable medical information and the content of their communications.

COUNT IV – IDENTITY THEFT

421. Plaintiffs incorporates all prior paragraphs as if fully stated herein.

422. 42 Pa.C.S. § 8315 provides that a victim of identity theft may bring a civil action based on violations of 18 Pa.C.S. § 4120 and “a court of competent jurisdiction may award damages as follows: (1) Actual damages arising from the incident or \$500, whichever is greater. Damages include loss of money, reputation, or property, whether real or personal. The court may, in its discretion, award up to three times the actual damages sustained, but not less than \$500; (2) Reasonable attorneys fees and costs; and (3) Additional relief the court deems necessary and proper.”

423. The Pennsylvania Identity Theft Statute, 18 Pa.C.S. § 4120, states that a person commits the offense of identity theft if he “uses, through any means, identifying information of another person without the consent of that person to further any unlawful purpose.”

424. Under the Pennsylvania Identity Theft Statute, “identifying information” means “[a]ny ... fact used to establish identity, including but not limited to, a name, birth date, Social Security number, driver’s license number, nondriver governmental identification number, telephone number, checking account number, savings account number, student identification number, employee or payroll number or electronic signature.”

425. Patient IP addresses and unique persistent cookie and device identifiers are “identifying information” because they are facts used to establish identity by the third parties that Defendant procured to acquire and record patient communications for marketing purposes without Plaintiffs or patient Class members’ knowledge, consent, authorization, or any further action.

426. Some of the persistent cookie identifiers, IP address, and browser identifiers

used by UPMC in conjunction with its deployment of third-party source code are more precise “identifying information” than a name. For example, there are several Mark Zuckerbergs in the world, but there’s only one Mark Zuckerberg with a c_user cookie identifier of 4.

427. Defendant used Plaintiffs’ and patient Class members’ IP addresses and unique, persistent cookie identifiers and device identifiers for the following unlawful purposes:

- a. To procure the third parties detailed herein to acquire and record the content of Plaintiffs’ and patient Class members’ communications exchanged with Defendant in violation of the Pennsylvania Wiretapping and Electronic Surveillance Control Act;
- b. To knowingly use the contents of the communications intercepted by the third parties procured by Defendant in violation of the Pennsylvania Wiretapping and Electronic Surveillance Control Act for marketing purposes;
- c. To engage in the unlawful use of a computer under 18 Pa. C.S.A. § 7611(1) by taking control of Plaintiffs’ and Class members’ computing devices through source code that commandeered said devices and caused the transmission of patient identifiers and the contents of patient communications to the third parties as detailed herein by means of false or fraudulent pretenses, representations, or promises as detailed above;
- d. To engage in the unlawful use of a computer under 18 Pa.C.S.A. § 7611(3) by giving identifying codes, personal identification numbers, and other confidential information about the computers of Plaintiffs and Class members to third parties;

- e. To engage in unlawful duplication under 18 Pa.C.S.A. § 7614 by making or causing to be made an unauthorized copy, in any form, of computer data that resided in, was communicated by, and produced by Plaintiffs and patient Class members' computers; and
- f. To engage in violations of the Pennsylvania Trade and Unfair Business Practices Act as alleged herein.

428. As a direct and proximate cause of Defendant's unauthorized use of Plaintiffs' and patient Class members' identifying information to further the unlawful purposes described herein, Plaintiffs and Class members were damaged by Defendant's breach in that:

- a. Sensitive and confidential information that Plaintiffs and Class members intended to remain private is no more;
- b. Defendant eroded the essential confidential nature of the provider-patient relationship;
- c. Defendant took something of value from Plaintiffs and Class members and derived benefit therefrom without Plaintiffs' and Class members' knowledge or informed consent and without sharing the benefit of such value;
- d. Plaintiffs and Class members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- e. Defendant's actions diminished the value of Plaintiffs' and Class members' personal information; and
- f. Defendant's actions violated the property rights Plaintiffs and patients have in their personally identifiable medical information and the content of their communications.

COUNT V – NEGLIGENT MAINTENANCE OF PATIENT DATA

429. Plaintiffs incorporate all prior paragraphs as if fully stated herein.

430. Defendant had a duty to keep patient data and communications in the strictest

confidence and to enact adequate safeguards for the personal identifiable information of Plaintiffs and other patient Class members.

431. Regardless of its status as Plaintiffs' and patient Class members' medical provider, Defendant undertook such duty when it promised, among other things, to "safeguard [patient] personal information" and that it would "keep the personal information of [its] patients in the strictest confidence."

432. Defendant breached that duty by deploying third party source code at UPMC.com and myupmc.upmc.com that it knew, or should have known, would cause the disclosure of personally identifiable data and communications about patients to several third parties.

433. As a direct and proximate cause of Defendant's unauthorized use of Plaintiffs and Class members' identifying information to further the unlawful purposes described herein, Plaintiffs and Class members were damaged by Defendant's breach in that:

- a. Sensitive and confidential information that Plaintiffs and Class members intended to remain private is no more;
- b. Defendant eroded the essential confidential nature of the provider-patient relationship;
- c. Defendant took something of value from Plaintiff and Class members and derived benefit therefrom without Plaintiff and Class members knowledge or informed consent and without sharing the benefit of such value;
- d. Plaintiffs and Class members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- e. Defendant's actions diminished the value of Plaintiffs and Class members personal information; and
- f. Defendant's actions violated the property rights Plaintiffs and patients have in their personally identifiable medical information and the content of their communications.

COUNT VI – INTRUSION UPON SECLUSION

434. Plaintiffs incorporate all prior paragraphs as if fully stated herein.

435. Pennsylvania has recognized a privacy interest under common law, specifically at Restatement (Second) of Torts § 652B, “Intrusion upon Seclusion,” which states: “One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another in his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.”

436. Patients have a right of solitude or seclusion in the personally identifiable data and communications exchanged with their health care providers.

437. Defendant intruded upon Plaintiffs’ and Class members’ rights to solitude and seclusion by deploying source code that disclosed and caused transmissions of patient personally identifiable data and communications to dozens of third parties, effectively inviting the third parties into Plaintiffs’ and Class members’ private and secluded data and space.

438. Defendant’s intrusion violated its statutory duties to patients.

439. Defendant’s intrusion violates its common law duties to patients.

440. Defendant’s intrusions constituted violations of criminal laws, including unauthorized electronic surveillance, identity theft, unlawful use of a computer, and unlawful duplication.

441. Defendant’s intrusions violated the express promises Defendant made to Plaintiffs and patient Class members.

442. Defendant’s intrusions and breach of privacy of its own patients would be highly offensive to reasonable persons.

443. As a direct and proximate cause of Defendant’s unauthorized use of Plaintiffs’ and

Class members' identifying information to further the unlawful purposes described herein, Plaintiffs and Class members were damaged by Defendant's breach in that:

- a. Sensitive and confidential information that Plaintiffs and Class members intended to remain private is no more;
- b. Defendant eroded the essential confidential nature of the provider-patient relationship;
- c. Defendant took something of value from Plaintiffs and Class members and derived benefit therefrom without Plaintiffs' and Class members' knowledge or informed consent and without sharing the benefit of such value;
- d. Plaintiffs and Class members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- e. Defendant's actions diminished the value of Plaintiffs' and Class members' personal information; and
- f. Defendant's actions violated the property rights Plaintiffs and Class members have in their personally identifiable medical information and the content of their communications.

PRAYER FOR RELIEF

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

- a. General damages for the violation of privacy in an amount to be determined by a jury without reference to specific harm;
- b. Statutory damages of \$1,000 pursuant to 18 Pa.C.S.A. § 5725(a)(1);
- c. Statutory damages of \$500 pursuant to 18 Pa.C.S. § 4120;
- d. Statutory damages of \$100 for violation of the 73 P.S. § 201-9.2;
- e. A reasonable royalty for Defendant's misappropriation of personally identifiable patient data and communications;

- f. Imposition of a constructive trust against Defendant through which Plaintiffs can be compensated for any unjust enrichment gained by Defendant;
- g. Nominal damages for violation of Plaintiffs' and Class members' legal rights;
- h. The value of the data Defendant disclosed and used without Plaintiffs' and other patients' authorization;
- i. Attorneys' fees and litigation costs reasonably expended; and
- j. Punitive damages in an amount to be determined by a jury.

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

DEMAND FOR JURY TRIAL

Plaintiffs hereby make demand for trial by jury on all issues so triable.

Respectfully submitted,

By: 

James C. Shah (PA ID No. 80337)

Nathan Zipperian (PA ID No. 202585)

Michael Ols (PA ID No. 326144)

SHEPHERD, FINKELMAN, MILLER &
SHAH, LLP

1845 Walnut Street, Suite 806

Philadelphia, PA 19103

Telephone: (610) 891-9880

Facsimile: (866) 300-7367

jshah@sfmslaw.com

nzipperian@sfmslaw.com

mols@sfmslaw.com

Jay Barnes
Mitchell Breit
SIMMONS HANLY CONROY
112 Madison Avenue
New York, New York 10016-7416
Telephone: (212) 784-6400
Facsimile: (212) 213-5949
jaybarnes@simmonsfirm.com
mbreit@simmonsfirm.com

*Attorneys for Plaintiffs and the Proposed
Class*

VERIFICATION

I, James C. Shah, hereby state that I am counsel for the Plaintiffs; that I am authorized to make this verification on behalf of Plaintiffs in the foregoing action; that I have personal knowledge of the statements made in the foregoing Complaint; and that the statements made in Plaintiffs' Complaint are true and correct to the best of my knowledge, information and belief.

I understand that the statements in this Verification are subject to the penalties of 18 Pa.C.S. § 4904 relating to unsworn falsification to authorities.

Dated: 1/23/2020



James C. Shah

PLAINTIFFS' EXHIBIT 1

UPMC's Notice of Privacy Practices - Pittsburgh, PA



UPMC's Notice of Privacy Practices

Effective Date: November 14, 2018

- [List of Entities Covered by UPMC's Notice of Privacy Practices](#)
- [Full Notice](#)
- [Notice of Privacy Practices \(PDF\)](#)
- [ClinicalConnect HIE Standard Addendum to the Notice of Privacy Practices \(PDF\)](#)

Summary

At UPMC, we are committed to protecting the privacy of your medical information, as federal and state laws require. When we say “information,” we mean health, treatment, or payment information that identifies you. Attached is UPMC’s “Notice of Privacy Practices.” The Notice explains how we meet this commitment. The Notice also explains your legal rights about what is in your health record. All people and places that make up UPMC must follow the Notice. However, this does not include UPMC Health Plan or UPMC as an employer. This Summary tells you in brief what the Notice says. **This summary is not a complete listing of how we use and disclose (share) your health information. If you have a question about any of the information in this summary, you should review the full Notice of Privacy Practices or ask a UPMC staff member for more information.** UPMC has the right to change this Summary and the Notice without first notifying you.

How UPMC may use and share your health information

Without your consent, UPMC can use and share your health information to:

- Provide you with medical treatment and other services.
- Receive payment from you, an insurance company, or someone else for services we provide to you.
- Coordinate your care, which may include such things as giving you appointment reminders and telling you about other treatment options.
- Contact you for certain marketing and fundraising activities, unless otherwise indicated by you.
- Comply with the law.
- Meet special situations as described in the Notice, such as public health, safety, and research.

Unless you object, UPMC can:

- Include your name and other information in the hospital directory.
- Share your health information with a family member or a close personal friend.

All other uses and sharing of your health information will be done only with your specific written permission or as required by law.

Your legal rights about your health information

- Right to ask to see and request a copy of your medical record
- Right to ask that incorrect or incomplete information in your medical record be corrected
- Right to ask for a list of all people and organizations who UPMC disclosed your health information to, subject to limits permitted by law

- Right to ask UPMC to limit how we use and share your health information without your consent
- Right to ask for confidential communications
- Right to ask for a paper copy of the Notice of Privacy Practices

Violation of privacy rights

If you believe your privacy rights have been violated, you have a right to file a complaint. Please see UPMC's Notice of Privacy Practices for more details.

In the event that a breach of your protected health information occurs at UPMC or one of its Business Associates, you will be provided written notification as required by law.

Full Notice

This notice describes how medical information about you may be used and disclosed (shared) and how you can get access to (see and copy) this information.

Please review it carefully.

Background

UPMC creates and maintains a record of information about the care and services you receive at UPMC. This includes information that UPMC receives from other doctors and medical facilities that are not part of UPMC, but that UPMC keeps to help give you better care. UPMC may share and use your health information for purposes of treating you, obtaining payment for services provided to you, health care operations as described in this Notice, as well as purposes authorized by you or permitted by law. You can learn more about UPMC at www.upmc.com.

What Is a Notice of Privacy Practices?

The Notice tells you about the ways we may use and share your health information, as well as the legal duties we have about your health information. The Notice also tells you about your rights under federal (United States) and state (Pennsylvania) laws. In this Notice, the words "we," "us," and "our" mean UPMC and all the people and places that make up UPMC. This Notice does not apply to the UPMC Health Plan or UPMC as an employer.

Who Follows UPMC's Notice of Privacy Practices?

A list of entities that are bound by this Notice can be found within the privacy information section of www.upmc.com. This includes hospitals, doctors, rehabilitation services, skilled nursing services, home health services, pharmacy services, laboratory services, and other related health care providers. This also includes departments, units, and staff within our health care facilities, health care professionals permitted by us to provide services to you, and students, residents, trainees, volunteers, and others involved in providing your care whether or not these individuals are employed by UPMC.

This Notice does not apply to the UPMC Health Plan or UPMC as an employer. These UPMC entities are separate covered entities for the purpose of the Health Insurance Portability and Accountability Act (HIPAA) and have their own Notice. Additionally, if your doctor is not a member of a physician practice that is owned by UPMC, he or she may have different policies about how to handle your information and will have a separate Notice.

Our Duty to Protect Your Health Information

We are required by law to:

- Make sure that information that identifies you is kept private and is used in accordance with this notice (as currently in effect).
- Make available to you this Notice that describes the ways we use and share your health information as well as your rights under the law about your health information.

How We May Use and Share Your Health Information with Others

The law permits us to use and share your health information in certain ways. When we act in response to your written permission, share information to help treat you, or are directed by the law, we will share all information that you, your health care provider, or the law permits or requires. The list below tells you about different ways that we may use your health information and/or share it with others. We have also provided you with examples of what we mean. Every possible example of how we may use or share information is not listed below. However, all of the ways we are permitted to use and share information fall into one of the groups below. When possible, we will use health information that does not identify you.

A. Ways We Are Allowed to Use and Share Your Health Information With Others Without Your Consent or as the UPMC Consent for Treatment, Payment, and Health Care Operations Provides:

1. **Treatment.** We may use your health information to give you medical treatment or services. We may also share your health information with people and places that provide treatment to you. For example, if you have diabetes, the doctor may need to tell the dietitian about your diabetes so that you get the kind of meals you need. We may share health information about you with people outside of UPMC who provide follow-up care to you, such as your physicians, other providers, EMS providers, nursing homes and home care agencies. At all times, we will comply with any regulations that apply.
2. **Payment.** In order to receive payment for the services we provide to you, we may use and share your health information with your insurance company or a third party. We also may share your health information with other health care service or product providers who provide follow-up care to you, such as your physicians, other providers, EMS providers, nursing homes and home care agencies so they can bill you, your insurance company, or a third party. For example, some health plans require your health information to pre-approve you for surgery and require pre-approval before they pay us.
3. **Health Care Operations.** We may use and share your health information so that we, or others that have provided treatment to you, can better operate the office or facility. For example, we may use your health information to review the treatment and services we gave you and to see how well our staff cared for you. We may share your health information with our researchers, so they can develop plans to conduct research. We may share information with our students, trainees, and staff for review and learning purposes. We may share your information for case management and care coordination purposes. We will not sell your name or any identifiable health information to others without your authorization.
4. **Health Information Exchanges.** We may share your information using a variety of Health Information Exchanges both on a regional and a national basis. You have the right not to participate in these exchanges. If you choose not to participate in the exchanges, your health information will no longer be accessible through the exchange. However, it does not affect the information that was exchanged prior to the time you chose not to participate. You can learn more about the health information exchanges UPMC participates in at www.upmc.com.
5. **Business Associates.** We may share your health information with others called "business associates," who perform services on our behalf. The Business Associate must agree in writing to protect the confidentiality of the information. For example, we may share your health information with a billing company that bills for the services we provided.
6. **Appointment Reminders.** We may use and share your health information to remind you of your appointment for treatment or medical care. For example, if your doctor has sent you for a test, and you have approved communication, the place where the testing will be done may call, text, or e-mail you to remind you of the date you are scheduled.
7. **Appointment Confirmations.** We may use and share your health information to confirm the time, place and attendance of your appointment for treatment with third-party transportation services.

8. **Treatment Options and Other Health-Related Benefits and Services.** We may use and share your health information to tell you about possible treatment options and other health-related benefits and services that may interest you. For example, if you suffer from an illness or condition, we may tell you about a special treatment or research study that is being offered.
9. **Fundraising Activities.** We may use and share with a Business Associate or a foundation that is related to us your name, address, phone number, and other such information (called "demographic information"), the dates that health care was provided to you, general department information regarding the department where services were rendered, the name of your treating physician and outcome information. You may then be asked for a donation to UPMC. For example, you may receive a letter from a UPMC foundation asking for a donation to support enhanced patient care, treatment, education or research at UPMC. Any fund-raising materials will explain how you can tell us, a business associate, or a foundation that you do not want to be contacted in the future.
10. **Marketing Activities.** We may use or share your health information for marketing purposes without your permission when we discuss such products or services with you face to face or to provide you with an inexpensive promotional gift related to the product or service. For example, you may receive samples of products or drugs during a visit to a UPMC hospital or facility. For other types of marketing activities, we will obtain your written permission before using or sharing your health information. We will not sell your identifiable health information to others without authorization.
11. **Research.** We may use and share your health information for research 1) if our researcher obtains permission from a special UPMC committee that decides if the request meets certain standards required by law; or 2) if you provide us with your written permission to do so. You may participate in a research study that requires you to obtain hospital and other health care services. In this case, we may share the information that we create 1) to our researcher who ordered the hospital or other health care services; and 2) to your insurance company in order to receive payment for services that your insurance will pay for. We may use and share with a UPMC researcher your health information if certain parts of your information that would identify you, such as your name and other items that the law describes, are removed before we share it with the UPMC researcher. This will be done when the researcher signs a written agreement with us that the researcher will not share the information again, will not try to contact you, and will obey other requirements that the law provides. We may also share your health information with a Business Associate who will remove information that identifies you so that the remaining information can be used for research.
12. **Special Situations.** In the following situations, the law either permits or requires us to use or share your health information with others. Pennsylvania law may further limit these disclosures; for example, in cases of behavioral health information, drug and alcohol treatment information, and HIV status:
 - a. **As Required by Law.** We will share your health information when required by federal, state, or local law. For Example:
 - If we believe that you have been a victim of abuse, neglect, or domestic violence, we will share your health information with an authorized government agency. If we share your health information for this purpose, we will tell you unless we believe that telling you would put you or someone else at risk of harm.
 - b. **To Prevent a Serious Threat to Health or Safety.** We may use and share your health information with persons who may be able to prevent or lessen the threat or help the potential victim of the threat when doing so is necessary to prevent a serious threat to the health and safety of you, the public, or another person. Pennsylvania law may require such disclosure when an individual or group has been specifically identified as the target or potential victim.
 - c. **Organ and Tissue Donation.** To assist in the process of eye, organ or tissue transplants, in the event of your death, we may share your health information with organizations that obtain, store, or transplant eyes, organs, or tissue.

- d. **Special Government Purposes.** We may use and share your health information with certain government agencies, such as:
- **Military and Veterans.** We may share your health information with military authorities as the law permits if you are a member of the armed forces (of either the United States or a foreign government).
 - **National Security and Intelligence.** We may share your health information with authorized federal officials for intelligence, counter-intelligence and other national security activities authorized by law.
 - **Protective Services for the President and Others.** We may share your health information with authorized federal officials to protect the President of the United States, other authorized persons, or foreign heads of state. We may also share your health information for purposes of conducting special investigations as authorized by law.
- e. **Workers' Compensation.** We may share your health information for Workers' Compensation or similar programs that provide benefits for work-related injuries or illness.
- f. **Public Health.** We may share your health information with public health authorities for public health purposes to prevent or control disease, injury, or disability. This includes, but is not limited to, reporting disease, injury, and important events such as birth or death, and conducting public health monitoring, investigations, or activities. For example, we may share your health information to 1) report child abuse or neglect; 2) collect and report on the quality, safety, and effectiveness of products and activities regulated by the Food and Drug Administration (FDA) (such as drugs and medical equipment, and could include product recalls, repairs, and monitoring); or 3) notify a person who may have been exposed to or is at risk of spreading a disease.
- g. **Health Oversight.** We may share your health information with a health oversight agency for purposes including 1) monitoring the health care system; 2) determining benefit eligibility for Medicare, Medicaid, and other government benefit programs; and 3) monitoring compliance with government regulations and civil rights laws.
- h. **Coroners, Medical Examiners, and Funeral Directors.** We may share your health information with a coroner or medical examiner in order to identify a deceased person, determine the cause of death, or for other reasons allowed by law. We also may share your health information with funeral directors, as necessary, so they can carry out their duties.
- i. **Inmates.** If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may share your health information with the correctional institution or law enforcement official. This would be necessary 1) for the institution to provide you with health care; 2) to protect your health and safety or the health and safety of others; or 3) for the safety and security of the correctional institution and its staff.

B. Other Ways We Are Allowed to Use and Provide Your Health Information to Others

1. **Hospital Directory.** We may include limited information about you in the hospital directory while you are a patient at a UPMC hospital or other facility. The information may include your name, location in the building, general condition, such as "stable," "serious," "critical," and your religious affiliation. Except for your religious affiliation, the directory information may be released to people who ask for you by name. We may give your religious affiliation to a member of the clergy, such as a priest or rabbi, even if they don't ask for you by name. This helps your family, friends, and clergy who visit you to know how you are doing. You have the right to ask that all or part of your information not be given out. If you do so, we will not be able to tell your family or friends your room number or that you are in the hospital or facility.
2. **People Involved in Your Care or Payment for Your Care.** We may share your health information with a friend, family member, or another person identified by you who is involved in your medical care or the payment of your medical care. We may share your health information with these persons if you

are present or available before we share your health information with them and you do not object to our sharing your health information with them, or we reasonably believe that you would not object to this. If you are not present and certain circumstances indicate to us that it would be in your best interests to do so, we will share information with a friend or family member or someone else identified by you, to the extent necessary. This could include sharing information with your family or friend so that they could pick up a prescription or a medical supply. We may tell your family or friends that you are in a UPMC hospital and your general condition. We may share medical information about you with an organization assisting in a disaster relief effort.

3. Permissible Disclosures to Law Enforcement. We may share your health information with a law enforcement official or authorized individual:

- a. in response to a court order, subpoena, warrant, summons or similar process;
- b. to identify or locate a suspect, fugitive, material witness, or missing person;
- c. about the victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement;
- d. about a death we believe may be the result of criminal conduct;
- e. about criminal conduct at the hospital; or in emergency circumstances to report a crime; the location of the crime or victims;
- f. or the identity, description or location of the person who committed the crime.

4. Exception to the Above. If you are a patient in a psychiatric/mental/behavioral health facility or drug and alcohol facility, additional authorization may be required to release your information outside of UPMC. If you are under 14 years of age, this permission must come from your parents or legal guardians. If you are 14 years or older, this permission must come from you.

C. In All Other Ways, We Will Require Your Written Permission Before Your Health Information Is Used or Shared With Others

Except as stated in Sections A and B, your written permission is required before we can use or share your health information with anyone outside of UPMC. This permission is provided through a form. If you give us permission to use or share health information about you, you may cancel that permission, in writing, at any time. If you cancel your permission, we will no longer use or share your health information for the reasons you have given us in your written permission. However, we are unable to take back any information that we have already shared with your permission.

Your Rights Concerning Your Health Information

The law gives you the following rights about your health information:

- 1. Right to Ask to See and Request a Copy.** You have the right to ask to see and request a copy of the health information we used to make decisions about your care. This includes your right to request a copy of your electronic medical record in electronic form. Your request must be in writing and given to your doctor or the place where you were treated. You can call your doctor's office or the place where you were treated to find out how to do this. If you ask to see or request a copy of your health information, you may have to pay fees as permitted by law. We may tell you that you cannot see nor have a copy of some or all of your health information. If we tell you this, you may ask that someone else at UPMC review this decision. A licensed health care professional chosen by UPMC will review those that can be reviewed. This person will not be the same person who refused your request. We will do whatever this person decides.
- 2. Right to Ask for a Correction.** If you feel that health information we have about you is incorrect or incomplete, you may ask us to correct the information. You have the right to ask for a correction for as long as the information is kept by or for UPMC. You must put your request in writing and give it to your doctor or the place where you received care. If you do not ask in writing or give your reasons in writing, we may tell you that we will not do as you have asked. We have the right to refuse your request if 1) we determine that the information is correct and complete; 2) the information is not part of the health information created or

kept by or for UPMC; 3) the person or place who created the information is no longer available to make the correction and we believe the information to be correct; or 4) the information is not part of the information that you are permitted by law to see and/or copy.

3. **Right to Ask for an "Accounting of Disclosures."**

- a. **Generally.** You have the right to ask us for an "accounting of disclosures." This is a list of those people and organizations who have received or have accessed your health information. This right does not include information made available for treatment, payment, or health care operations, or made available when you have provided us with permission to do so. You must put your request in writing and give it to your doctor or the place where you received care. You can call your doctor's office or the place where you received care to find out how to ask for the list. You must include in your written request how far back in time you want us to go, which may not be longer than six years.
- b. **Information that is Maintained Electronically.** Subject to a schedule established by federal law, if we maintain your health information electronically (in our computer), you have the right to ask for an accounting of disclosures of where UPMC disclosed your health information. In accord with federal law, you may request an accounting for a period of three years prior to the date the accounting is requested. You also have the right to ask our business associates for an accounting of their disclosures. We will post a list of all of our business associates and how to contact them on our website.

4. **Right to Ask for Limits on Use and Sharing.**

- a. **Generally.** You have the right to ask us to limit the health information we use or share with others about you for treatment, payment, or health care operations. You also have the right to ask us to limit health information that we share with someone who is involved in your care or payment for your care, like a family member or friend. You can call your doctor's office or the place where you received your care to get instructions on how to submit such a request. In your request, you must tell us 1) what information you want to limit; 2) whether you want to limit our use, disclosure or both; and 3) the person or institution the limits apply to (for example, your spouse). For example, you could ask that we not use or share information about a surgery you had. You must put your request in writing and give it to your doctor or the place where you received your care. We are not required to agree to your request. If we do agree to your request, we still may provide information, as necessary, to give you emergency treatment.
- b. **Services Paid For by You.** Where you have paid for your services out of pocket in full, at your request, we will not share information about those services with a health plan for purposes of payment or health care operations. "Health plan" means an organization that pays for your medical care.

5. **Right to Ask for Confidential Communications.** You have the right to ask that we contact you about your health information in a certain way or at a certain location that you believe provides you with greater privacy. For example, you can ask that we contact you at work or by mail. Your request must state how or where you wish to be contacted. You must make your request in writing to your doctor or the place where you received care. You do not need to provide a reason for your request. We will comply with all reasonable requests.

6. **Right to Ask for a Paper Copy of This Notice.** You may ask us to give you a copy of this Notice at any time. Even if you have agreed to receive this Notice electronically (for example, through the computer), you still have the right to a paper copy of this Notice. You can also get a copy of this Notice at our website. To obtain a paper copy of this Notice, contact your doctor's office or the registration department of the place where you received care.

7. 8. UPMC Insurance Division is prohibited from requesting, requiring or purchasing genetic information with respect to any individual prior to such individual's enrollment in a health plan, and from using genetic information for underwriting purposes.

Violation of Privacy Rights

In the event that a breach of your protected health information occurs by UPMC or one of its Business Associates, you will be provided with written notification as required by law.

If you believe your privacy has been violated by us, you may file a confidential complaint directly with us. You can do this by contacting the UPMC Privacy Officer at the hospital or facility where you received care or by calling the UPMC Compliance Help Line at 1-877-983-8442, or the UPMC Office of Patient and Consumer Privacy at 412-647-5757.

You also may file a complaint with the Secretary of the U.S. Department of Health and Human Services. To file a complaint with the Secretary of Health and Human Services, you must 1) name the UPMC place or person that you believe violated your privacy rights and describe how that place or person violated your privacy rights; and 2) file the complaint within 180 days of when you knew or should have known that the violation occurred. All complaints to the Secretary of the U.S. Department of Health and Human Services must be in writing and addressed to:

U.S. Department of Health and Human Services
200 Independence Ave. S.W.
Washington, DC 20201

You will not be penalized for filing a complaint.

Changes to This Notice

We reserve (have) the right to change this Notice. We reserve (have) the right to make the revised or changed Notice effective for health information we already have about you and for any future health information. We will post a copy of the revised Notice in the places where we provide medical services and on our website. The Notice will contain the effective date on the first page, in the top right-hand corner. We will provide to you, if you ask us, a copy of the Notice that is currently in effect each time you register at UPMC as an inpatient or outpatient for treatment or health care services.

If You Have Questions About This Notice

If you have any questions about this Notice, please contact your doctor or the place where you received care. You also may contact **UPMC's Notice of Privacy inquiry line at 412-647-6286** or the **UPMC Office of Patient and Consumer Privacy at 412-647-5757**.

Entities Covered by UPMC's Notice of Privacy Practices

UPMC's Notice of Privacy Practices covers all organizations under the control of UPMC, including, but not limited to:

UPMC Hospitals

- [UPMC Presbyterian](#)
- [UPMC Shadyside](#)
- [UPMC Altoona](#)
- [UPMC East](#)
- [UPMC Bedford](#)
- [UPMC Hamot**](#)
- [UPMC Horizon – Greenville](#)
- [UPMC Horizon – Shenango Valley](#)
- [UPMC Jameson](#)
- [UPMC Kane](#)

- [UPMC McKeesport](#)
- [UPMC Mercy](#)
- [UPMC Montefiore](#)
- [UPMC Northwest](#)
- [UPMC Passavant–McCandless](#)
- [UPMC Passavant–Cranberry](#)
- [UPMC Pinnacle](#)
- [UPMC St. Margaret](#)
- [UPMC Susquehanna](#)
- [UPMC Children's Hospital of Pittsburgh](#)
-
- [UPMC Magee-Womens Hospital](#)
- [UPMC Western Psychiatric Hospital](#)

****Affiliated with UPMC Hamot**

- [Hamot Medical Center](#)
- [Hamot Primary Care Network](#)
- [Hamot Diabetes Institute](#)
- [Bayside Pharmacy \(Hamot\)](#)
- [Hamot Sports Medicine Center](#)
- [Great Lakes Home Healthcare \(Hamot\)](#)
- [Great Lakes Home Health Services \(Hamot\)](#)
- [Great Lakes Hospice \(Hamot\)](#)
- [Great Lakes Home Medical \(Hamot\)](#)

UPMC Hamot Joint Ventures

[The Regional Cancer Center](#)

UPMC Pinnacle

- UPMC Pinnacle Hospitals
 - West Shore Surgery Center, Ltd.
 - Concentra Occupational Healthcare Harrisburg, LP
 - Pinnacle Health Emergency Department Services, LLC
 - Pinnacle Health Hospitalists Services, LLC
 - Pinnacle Health Observation Services, LLC
 - UPMC Pinnacle Anesthesia Services, LLC
 - Susquehanna Valley Surgery Center, LLC
 - Walnut Bottom Radiology, LLC
- Pinnacle Health Medical Services
- Pinnacle Health Ventures, Inc.
 - Medcare Susquehanna Valley, LLC
 - Pinnacle Health Imaging, Inc.
 - Pinnacle Health ABC, LLC
- United Health Risk, Ltd.
- United Central Pennsylvania Reciprocal Risk Retention Group
- Concert, LLC
- Pinnacle Health Integrative Services, LLC
- UPMC Pinnacle Carlisle
- UPMC Pinnacle Lancaster

- Lancaster Emergency Medical Services Association
- UPMC Pinnacle Lititz
 - Lancaster Emergency Medical Services Association
- UPMC Pinnacle Memorial
- Pinnacle Health Regional Physicians
- Pennsylvania Psychiatric Institute
- Pinnacle Health Foundation
- Community Life Team, Inc.
- Pinnacle Health Cardiovascular Institute, Inc.
- Hanover Healthcare Plus, Inc.
 - UPMC Pinnacle Hanover
 - Cherry Tree Cancer Center LLP
 - Hanover Health Corporation
 - Hanover Surgicenter, LLC
 - Hanover Apothecary, Inc.
 - Littlestown Health Care Partnership, LLC

UPMC Susquehanna

- UPMC Susquehanna Hospitals
 - UPMC Susquehanna Williamsport Regional Medical Center
 - UPMC Susquehanna Divine Providence
 - UPMC Susquehanna Muncy
 - UPMC Susquehanna Soldiers + Sailors
 - UPMC Susquehanna Lock Haven
 - UPMC Susquehanna Sunbury
- Haven Skilled Rehab and Nursing
- Susquehanna Health Medical Group (SHMG)
- The Green Home Skilled Nursing & Rehabilitation
- Tioga Health Care Providers, Inc. (THCP)
- Williamsport Area Ambulance Cooperative (WAAC) d/b/a Susquehanna Regional EMS

UPMC Surgery Centers

- [UPMC Monroeville Surgery Center](#)
- [UPMC South Surgery Center](#)

Other UPMC Facilities & Entities

- [Center for Emergency Medicine \(STAT MedEvac\)](#)
- [Chartwell](#)
- Eye & Ear Institute
- [Mon Yough Community Services](#)
- Physician Services Division
- [Safe Harbor Behavioral Health](#)
- [UPMC Hillman Cancer Center](#)
- UPMC Community Provider Services
- [UPMC at Home](#)

Affiliates

- Credentialed Medical Staff Physicians
- UPMC Hillman Cancer Center joint ventures:

- [UPMC/HVHS Cancer Center \(PDF\)](#)
- [UPMC/Jameson Cancer Center \(PDF\)](#)
- [UPMC and The Washington Hospital Cancer Center \(PDF\)](#)
- [Mountain View Cancer Associates LLP – Arnold Palmer Pavilion \(PDF\)](#)
- [Butler Cancer Associates, Inc. \(PDF\)](#)
- [Butler Cancer Associates, Inc. – BHS Radiation Oncology \(PDF\)](#)

Skilled Nursing, Retirement, Assisted Living, Independent Living, and Long-term Care Freestanding Facilities

- [Asbury Heights](#)
- [Beatty Pointe Village](#) in Monroeville
- [Canterbury Place](#) in Pittsburgh
- [Community LIFE](#) McKeesport
- [Community LIFE](#) Homestead
- [Community LIFE](#) Tarentum
- [Community LIFE](#) East End
- [Cranberry Place](#) in Cranberry Township
- [Cumberland Crossing](#) in the North Hills
- [Cumberland Woods Village](#) in Allison Park
- [Hampton Fields Village](#) in Allison Park
- [Heritage Place](#) in Squirrel Hill
- [Lighthouse Pointe at Chapel Harbor](#) in Pittsburgh
- [Seneca Manor](#) in Verona
- [Seneca Place](#) in Penn Hills
- [Sherwood Oaks](#) in Cranberry Township
- [Strabane Woods](#) in Washington
- [Sugar Creek Station](#) in Franklin
- [Weatherwood Manor](#) in Greensburg
- [Vanadium Woods Village](#) in Scott Township

Organized Health Care Arrangements

- UPMC Insurance Services Arrangement
 - UPMC Health Plan
- Skilled Nursing Facility Arrangements
 - Asbury Atlantic Inc dba Springhill
 - Charles M. Morris Nursing & Rehabilitation Center / JAA
 - Manor Care of Monroeville PA, LLC d.b.a. ManorCare Health Services, Monroeville
 - Manor Care of Whitehall Borough, Pittsburgh PA LLC d.b.a. ManorCare Health Services, Whitehall Borough
 - Presbyterian Medical Center of Oakmont Inc. d.b.a. The Willows of Presbyterian Senior Care
 - Vincentian Collaborative System / Vincentian Home
 - Avalon Place – Lawrence County / New Castle
 - Avalon Springs Place – Mercer County / Mercer
 - Jameson Care Center – Lawrence County
 - Monroeville Operations LLC d/b/a Monroeville Rehabilitation & Wellness Center – Allegheny County / Monroeville
 - Murrys ville Operations LLC d/b/a Murrys ville Rehabilitation & Wellness Center – Allegheny County / Murrys ville
 - St. Paul's Homes – Mercer County / Greenville

- Redstone Highlands Healthcare Center (pending) – Allegheny County / Greensburg
- Redstone Presbyterian Seniorcare – Greensburg
- ManorCare Greentree of Pittsburgh, PA, LLC d/b/a ManorCare Health Services - Greentree
- ManorCare of Bethel Park PA, LLC d/b/a ManorCare Health Services – Bethel Park
- United Methodist Services For The Aging D.B.A. Asbury Health Center
- Saint Mary's Home of Erie d/b/a Saint Mary's at Asbury Ridge
- Saint Mary's Home of Erie d/b/a Saint Mary's East
- Twinbrook Medical Center - Erie PA, LLC, d/b/a ManorCare Health Services - Erie
- Oncology Services
 - Trinity Health System
 - Indiana Regional Medical

UPMC Health Information Exchange Participation

- Care Everywhere
- Carequality
- ClinicalConnect HIE
- Commonwell Health Alliance
- eHealth Exchange
- HEALTHeLINK
- KeyHIE
- Pennsylvania Patient Provider Network (P3N)
- Pennsylvania Prescription Drug Monitoring Program (PDMP)
- Pennsylvania Statewide Immunization Information System (PA-SIIS)
- Surescripts e-Prescribing

PLAINTIFFS' EXHIBIT 2

UPMC's Notice of Privacy Practices

UPMC’s Notice of Privacy Practices

Effective Date: November 14, 2018

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED (SHARED) AND HOW YOU CAN GET ACCESS TO (SEE AND COPY) THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY.

Background

UPMC creates and maintains a record of information about the care and services you receive at UPMC. This includes information that UPMC receives from other doctors and medical facilities that are not part of UPMC, but that UPMC keeps to help give you better care. UPMC may share and use your health information for purposes of treating you, obtaining payment for services provided to you, health care operations as described in this Notice, as well as purposes authorized by you or permitted by law. You can learn more about UPMC at www.upmc.com.

What Is a Notice of Privacy Practices?

The Notice tells you about the ways we may use and share your health information, as well as the legal duties we have about your health information. The Notice also tells you about your rights under federal (United States) and state (Pennsylvania) laws. In this Notice, the words “we,” “us,” and “our” mean UPMC and all the people and places that make up UPMC. This Notice does not apply to the UPMC Health Plan or UPMC as an employer.

Who Follows UPMC’s Notice of Privacy Practices? A list of entities that are bound by this Notice can be found within the privacy information section of www.upmc.com. This includes hospitals, doctors, rehabilitation services, skilled nursing services, home health services, pharmacy services, laboratory services, and other related health care providers. This also includes departments, units, and staff within our health care facilities, health care professionals permitted by us to provide services to you, and students, residents, trainees, volunteers, and others involved in providing your care whether or not these individuals are employed by UPMC.

This Notice does not apply to the UPMC Health Plan or UPMC as an employer. These UPMC entities are separate covered entities for the purpose of the Health Insurance Portability and Accountability Act (HIPAA) and have their own Notice. Additionally, if your doctor is not a member of a physician practice that is owned by UPMC, he or she may have different policies about how to handle your information and will have a separate Notice.

Our Duty to Protect Your Health Information

We are required by law to:

- Make sure that information that identifies you is kept private and is used in accordance with this notice (as currently in effect).
- Make available to you this Notice that describes the ways we use and share your health information as well as your rights under the law about your health information.

How We May Use and Share Your Health Information with Others

The law permits us to use and share your health information in certain ways. When we act in response to your written permission, share information to help treat you, or are directed by the law, we will share all information that you, your health care provider, or the law permits or requires. The list below tells you about different ways that we may use your health information and/or share it with others. We have also provided you with examples of what we mean. Every possible example of how we may use or share information is not listed below. However, all of the ways we are permitted to use and share information fall into one of the groups below. When possible, we will use health information that does not identify you.

A. Ways We Are Allowed to Use and Share Your Health Information With Others Without Your Consent or as the UPMC Consent for Treatment, Payment, and Health Care Operations Provides:

1. **Treatment.** We may use your health information to give you medical treatment or services. We may also share your health information with people and places that provide treatment to you. For example, if you have diabetes, the doctor may need to tell the dietitian about your diabetes so that you get the kind of meals you need. We may share health information about you with people outside of UPMC who provide follow-up care to you, such as your physicians, other providers, EMS providers, nursing homes and home care agencies. At all times, we will comply with any regulations that apply.
2. **Payment.** In order to receive payment for the services we provide to you, we may use and share your health information with your insurance company or a third party. We also may share your health information with other health care service or product providers who provide follow-up care to you, such as your physicians, other providers, EMS providers, nursing homes and home care agencies so they can bill you, your insurance company, or a third party. For example, some health plans require your health information to pre-approve you for surgery and require pre-approval before they pay us.
3. **Health Care Operations.** We may use and share your health information so that we, or others that have provided treatment to you, can better operate the office or facility. For example, we may use your health information to review the treatment and services we gave you and to see how well our staff cared for you. We may share your health information with our researchers, so they can develop plans to conduct research. We may share information with our students, trainees, and staff for review and learning purposes. We may share your information for case management and care coordination purposes. We will not sell your name or any identifiable health information to others without your authorization.
4. **Health Information Exchanges.** We may share your information using a variety of Health Information Exchanges both on a regional and a national basis. You have the right not to participate in these exchanges. If you choose not to participate in the exchanges, your health information will no longer be accessible through the exchange. However, it does not affect the information that was exchanged prior to the time you chose not to participate. You can learn more about the health information exchanges UPMC participates in at www.upmc.com.
5. **Business Associates.** We may share your health information with others called “business associates,” who perform services on our behalf. The Business Associate must agree in writing to protect the confidentiality of the information. For example, we may share your health information with a billing company that bills for the services we provided.
6. **Appointment Reminders.** We may use and share your health information to remind you of your appointment for treatment or medical care. For example, if your doctor has sent you for a test, and you have approved communication, the place where the testing will be done may call, text, or e-mail you to remind you of the date you are scheduled.
7. **Appointment Confirmations.** We may use and share your health information to confirm the time, place and attendance of your appointment for treatment with third-party transportation services.



UPMC is an equal opportunity employer. Policy prohibits discrimination on the basis of race, color, religion, national origin, ancestry, sex, age, marital status, familial status, sexual orientation, disability, or veteran status. Further, UPMC will continue to support and promote equal employment opportunity, human dignity, and racial, ethnic, and cultural diversity. This policy applies to admissions, employment, and access to and treatment in UPMC programs and activities. This commitment is made by UPMC in accordance with federal, state and/or local laws and regulations.

UPMC’s Notice of Privacy Practices (continued)

Effective Date: November 14, 2018

8. Treatment Options and Other Health-Related Benefits and Services. We may use and share your health information to tell you about possible treatment options and other health-related benefits and services that may interest you. For example, if you suffer from an illness or condition, we may tell you about a special treatment or research study that is being offered.

9. Fundraising Activities. We may use and share with a Business Associate or a foundation that is related to us your name, address, phone number, and other such information (called “demographic information”) , the dates that health care was provided to you, general department information regarding the department where services were rendered, the name of your treating physician and outcome information. You may then be asked for a donation to UPMC. For example, you may receive a letter from a UPMC foundation asking for a donation to support enhanced patient care, treatment, education or research at UPMC. Any fund-raising materials will explain how you can tell us, a business associate, or a foundation that you do not want to be contacted in the future.

10. Marketing Activities. We may use or share your health information for marketing purposes without your permission when we discuss such products or services with you face to face or to provide you with an inexpensive promotional gift related to the product or service. For example, you may receive samples of products or drugs during a visit to a UPMC hospital or facility. For other types of marketing activities, we will obtain your written permission before using or sharing your health information. We will not sell your identifiable health information to others without authorization.

11. Research. We may use and share your health information for research 1) if our researcher obtains permission from a special UPMC committee that decides if the request meets certain standards required by law; or 2) if you provide us with your written permission to do so. You may participate in a research study that requires you to obtain hospital and other health care services. In this case, we may share the information that we create 1) to our researcher who ordered the hospital or other health care services; and 2) to your insurance company in order to receive payment for services that your insurance will pay for. We may use and share with a UPMC researcher your health information if certain parts of your information that would identify you, such as your name and other items that the law describes, are removed before we share it with the UPMC researcher. This will be done when the researcher signs a written agreement with us that the researcher will not share the information again, will not try to contact you, and will obey other requirements that the law provides. We may also share your health information with a Business Associate who will remove information that identifies you so that the remaining information can be used for research.

12. Special Situations. In the following situations, the law either permits or requires us to use or share your health information with others. Pennsylvania law may further limit these disclosures; for example, in cases of behavioral health information, drug and alcohol treatment information, and HIV status:

a. As Required by Law. We will share your health information when required by federal, state, or local law. For Example:

- If we believe that you have been a victim of abuse, neglect, or domestic violence, we will share your health information with an authorized government agency. If we share your health information for this purpose, we will tell you unless we believe that telling you would put you or someone else at risk of harm.

b. To Prevent a Serious Threat to Health or Safety. We may use and share your health information with persons who may be able to prevent or lessen the threat or help the potential victim of the threat when doing so is necessary to prevent a serious threat to the health and safety of you, the public, or another person. Pennsylvania law may require such disclosure when an individual or group has been specifically identified as the target or potential victim.

c. Organ and Tissue Donation. To assist in the process of eye, organ or tissue transplants, in the event of your death, we may share your health information with organizations that obtain, store, or transplant eyes, organs, or tissue.

d. Special Government Purposes. We may use and share your health information with certain government agencies, such as:

- **Military and Veterans.** We may share your health information with military authorities as the law permits if you are a member of the armed forces (of either the United States or a foreign government).

- **National Security and Intelligence.** We may share your health information with authorized federal officials for intelligence, counter-intelligence and other national security activities authorized by law.

- **Protective Services for the President and Others.** We may share your health information with authorized federal officials to protect the President of the United States, other authorized persons, or foreign heads of state. We may also share your health information for purposes of conducting special investigations as authorized by law.

e. Workers’ Compensation. We may share your health information for Workers’ Compensation or similar programs that provide benefits for work-related injuries or illness.

f. Public Health. We may share your health information with public health authorities for public health purposes to prevent or control disease, injury, or disability. This includes, but is not limited to, reporting disease, injury, and important events such as birth or death, and conducting public health monitoring, investigations, or activities. For example, we may share your health information to 1) report child abuse or neglect; 2) collect and report on the quality, safety, and effectiveness of products and activities regulated by the Food and Drug Administration (FDA) (such as drugs and medical equipment, and could include product recalls, repairs, and monitoring); or 3) notify a person who may have been exposed to or is at risk of spreading a disease.

g. Health Oversight. We may share your health information with a health oversight agency for purposes including 1) monitoring the health care system; 2) determining benefit eligibility for Medicare, Medicaid, and other government benefit programs; and 3) monitoring compliance with government regulations and civil rights laws.

UPMC’s Notice of Privacy Practices (continued)

Effective Date: November 14, 2018

- h. Coroners, Medical Examiners, and Funeral Directors.** We may share your health information with a coroner or medical examiner in order to identify a deceased person, determine the cause of death, or for other reasons allowed by law. We also may share your health information with funeral directors, as necessary, so they can carry out their duties.
- i. Inmates.** If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may share your health information with the correctional institution or law enforcement official. This would be necessary 1) for the institution to provide you with health care; 2) to protect your health and safety or the health and safety of others; or 3) for the safety and security of the correctional institution and its staff.

B. Other Ways We Are Allowed to Use and Provide Your Health Information to Others

- 1. Hospital Directory.** We may include limited information about you in the hospital directory while you are a patient at a UPMC hospital or other facility. The information may include your name, location in the building, general condition, such as “stable,” “serious,” “critical,” and your religious affiliation. Except for your religious affiliation, the directory information may be released to people who ask for you by name. We may give your religious affiliation to a member of the clergy, such as a priest or rabbi, even if they don’t ask for you by name. This helps your family, friends, and clergy who visit you to know how you are doing. You have the right to ask that all or part of your information not be given out. If you do so, we will not be able to tell your family or friends your room number or that you are in the hospital or facility.
- 2. People Involved in Your Care or Payment for Your Care.** We may share your health information with a friend, family member, or another person identified by you who is involved in your medical care or the payment of your medical care. We may share your health information with these persons if you are present or available before we share your health information with them and you do not object to our sharing your health information with them, or we reasonably believe that you would not object to this. If you are not present and certain circumstances indicate to us that it would be in your best interests to do so, we will share information with a friend or family member or someone else identified by you, to the extent necessary. This could include sharing information with your family or friend so that they could pick up a prescription or a medical supply. We may tell your family or friends that you are in a UPMC hospital and your general condition. We may share medical information about you with an organization assisting in a disaster relief effort.
- 3. Permissible Disclosures to Law Enforcement.** We may share your health information with a law enforcement official or authorized individual:
 - a.** in response to a court order, subpoena, warrant, summons or similar process;
 - b.** to identify or locate a suspect, fugitive, material witness, or missing person;
 - c.** about the victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement;
 - d.** about a death we believe may be the result of criminal conduct;

- e.** about criminal conduct at the hospital; or in emergency circumstances to report a crime; the location of the crime or victims;
- f.** or the identity, description or location of the person who committed the crime.

- 4. Exception to the Above.** If you are a patient in a psychiatric/mental/behavioral health facility or drug and alcohol facility, additional authorization may be required to release your information outside of UPMC. If you are under 14 years of age, this permission must come from your parents or legal guardians. If you are 14 years or older, this permission must come from you.

- C. In All Other Ways, We Will Require Your Written Permission Before Your Health Information Is Used or Shared With Others** Except as stated in Sections A and B, your written permission is required before we can use or share your health information with anyone outside of UPMC. This permission is provided through a form. If you give us permission to use or share health information about you, you may cancel that permission, in writing, at any time. If you cancel your permission, we will no longer use or share your health information for the reasons you have given us in your written permission. However, we are unable to take back any information that we have already shared with your permission.

Your Rights Concerning Your Health Information

The law gives you the following rights about your health information:

- 1. Right to Ask to See and Request a Copy.** You have the right to ask to see and request a copy of the health information we used to make decisions about your care. This includes your right to request a copy of your electronic medical record in electronic form. Your request must be in writing and given to your doctor or the place where you were treated. You can call your doctor’s office or the place where you were treated to find out how to do this. If you ask to see or request a copy of your health information, you may have to pay fees as permitted by law. We may tell you that you cannot see nor have a copy of some or all of your health information. If we tell you this, you may ask that someone else at UPMC review this decision. A licensed health care professional chosen by UPMC will review those that can be reviewed. This person will not be the same person who refused your request. We will do whatever this person decides.
- 2. Right to Ask for a Correction.** If you feel that health information we have about you is incorrect or incomplete, you may ask us to correct the information. You have the right to ask for a correction for as long as the information is kept by or for UPMC. You must put your request in writing and give it to your doctor or the place where you received care. If you do not ask in writing or give your reasons in writing, we may tell you that we will not do as you have asked. We have the right to refuse your request if 1) we determine that the information is correct and complete; 2) the information is not part of the health information created or kept by or for UPMC; 3) the person or place who created the information is no longer available to make the correction and we believe the information to be correct; or 4) the information is not part of the information that you are permitted by law to see and/or copy.

UPMC’s Notice of Privacy Practices (continued)

Effective Date: November 14, 2018

3. Right to Ask for an "Accounting of Disclosures."

- a. **Generally.** You have the right to ask us for an “accounting of disclosures.” This is a list of those people and organizations who have received or have accessed your health information. This right does not include information made available for treatment, payment, or health care operations, or made available when you have provided us with permission to do so. You must put your request in writing and give it to your doctor or the place where you received care. You can call your doctor’s office or the place where you received care to find out how to ask for the list. You must include in your written request how far back in time you want us to go, which may not be longer than six years.
- b. **Information that is Maintained Electronically.** Subject to a schedule established by federal law, if we maintain your health information electronically (in our computer), you have the right to ask for an accounting of disclosures of where UPMC disclosed your health information. In accord with federal law, you may request an accounting for a period of three years prior to the date the accounting is requested. You also have the right to ask our business associates for an accounting of their disclosures. We will post a list of all of our business associates and how to contact them on our website.

4. Right to Ask for Limits on Use and Sharing.

5. **Generally.** You have the right to ask us to limit the health information we use or share with others about you for treatment, payment, or health care operations. You also have the right to ask us to limit health information that we share with someone who is involved in your care or payment for your care, like a family member or friend. You can call your doctor’s office or the place where you received your care to get instructions on how to submit such a request. In your request, you must tell us 1) what information you want to limit; 2) whether you want to limit our use, disclosure or both; and 3) the person or institution the limits apply to (for example, your spouse). For example, you could ask that we not use or share information about a surgery you had. You must put your request in writing and give it to your doctor or the place where you received your care. We are not required to agree to your request. If we do agree to your request, we still may provide information, as necessary, to give you emergency treatment.
- a. **Services Paid For by You.** Where you have paid for your services out of pocket in full, at your request, we will not share information about those services with a health plan for purposes of payment or health care operations. “Health plan” means an organization that pays for your medical care.

6. **Right to Ask for Confidential Communications.** You have the right to ask that we contact you about your health information in a certain way or at a certain location that you believe provides you with greater privacy. For example, you can ask that we contact you at work or by mail. Your request must state how or where you wish to be contacted. You must make your request in writing to your doctor or the place where you received care. You do not need to provide a reason for your request. We will comply with all reasonable requests.

7. **Right to Ask for a Paper Copy of This Notice.** You may ask us to give you a copy of this Notice at any time. Even if you have agreed to receive this Notice electronically (for example, through the computer), you still have the right to a paper copy of this Notice. You can also get a copy of this Notice at our website. To obtain a paper copy of this Notice, contact your doctor’s office or the registration department of the place where you received care.
8. **UPMC Insurance Division is prohibited from requesting, requiring or purchasing genetic information with respect to any individual prior to such individual’s enrollment in a health plan, and from using genetic information for underwriting purposes.**

Violation of Privacy Rights

In the event that a breach of your protected health information occurs by UPMC or one of its Business Associates, you will be provided with written notification as required by law.

If you believe your privacy has been violated by us, you may file a confidential complaint directly with us. You can do this by contacting the UPMC Privacy Officer at the hospital or facility where you received care or by calling the UPMC Compliance Help Line at 1-877-983-8442, or the UPMC Office of Patient and Consumer Privacy at 412-647-5757.

You also may file a complaint with the Secretary of the U.S. Department of Health and Human Services. To file a complaint with the Secretary of Health and Human Services, you must 1) name the UPMC place or person that you believe violated your privacy rights and describe how that place or person violated your privacy rights; and 2) file the complaint within 180 days of when you knew or should have known that the violation occurred. All complaints to the Secretary of the U.S. Department of Health and Human Services must be in writing and addressed to:

U.S. Department of Health and Human Services 200
Independence Ave. S.W.
Washington, DC 20201

You will not be penalized for filing a complaint.

Changes to This Notice

We reserve (have) the right to change this Notice. We reserve (have) the right to make the revised or changed Notice effective for health information we already have about you and for any future health information. We will post a copy of the revised Notice in the places where we provide medical services and on our website. The Notice will contain the effective date on the first page, in the top right-hand corner. We will provide to you, if you ask us, a copy of the Notice that is currently in effect each time you register at UPMC as an inpatient or outpatient for treatment or health care services.

If You Have Questions About This Notice

If you have any questions about this Notice, please contact your doctor or the place where you received care. You also may contact **UPMC’s Notice of Privacy inquiry line at 412-647-6286** or the **UPMC Office of Patient and Consumer Privacy at 412-647-5757**

PLAINTIFFS' EXHIBIT 3

MyUPMC: A Free Online Patient Health Portal



Name

Sex

DOB

PCP

Terms and Conditions

Website/Email Terms of Use



MyUPMC Terms and Conditions



MyUPMC Terms and Conditions

Terms and Conditions

These terms apply to UPMC's websites and apps, including the websites and apps for MyUPMC.

If there are additional terms associated with a specific UPMC website or app, you will be presented with those additional terms at the time you access the website or app. However, those additional terms will apply only to that particular website or app. Collectively, all these terms constitute an agreement between UPMC and you.

UPMC controls our websites and apps from our offices in Pittsburgh, Pennsylvania, USA. By accessing our websites and apps, you agree that your access and use are governed by and will be interpreted in accordance with these terms of use and the laws of the Commonwealth of Pennsylvania, USA, without regard to conflict of laws principles.

These terms, materials referenced in these terms, and the content of the UPMC websites and apps are subject to change at UPMC's sole discretion. Any changes made are effective upon posting. It is your responsibility to review these terms of use each time you access a UPMC website or app, because you will be bound by any changes made.

General Website Disclaimer

- *If you think that you may have a medical emergency, call emergency medical services immediately (911) or go to a hospital Emergency Department. If you are seeking a referral or consultation with a medical expert, please contact the UPMC Consumer Referral Service, Monday through Friday, 9 a.m. to 5 p.m., at 1-800-533 - UPMC (8762).*

- UPMC's websites and apps are designed for general patient and member educational and informational purposes only. The information presented describes the products and services offered by UPMC using general terms to improve comprehension.
 - With respect to medical information, other than information provided to you by your provider through direct communication, or based on an online care appointment, information made available by UPMC through a website or an app should not be construed as an offer for medical services or as medical advice.
 - With respect to other products and services (including products available through the UPMC Health Plan), general terms may be used to improve comprehension. While some specific information may be provided, the information presented on our webpages and apps may not contain all the applicable terms, conditions, limitations, or exclusions necessary to fully describe the products and services being described. product and/or service descriptions are not intended to constitute offers to sell or solicitations in connection with any product or service. Information about the specific terms, conditions, limitations, or exclusions for a specific product or service available through UPMC is fully described in the additional materials available from UPMC.
- UPMC's websites and apps are designed to supplement — not replace — the relationship you have with your health care provider. Without limitation, UPMC does not recommend or endorse any specific tests, non-UPMC providers, medications, products, or procedures. UPMC asks that you consult a qualified health care professional for any diagnosis or treatment, including information regarding which medications or treatments are safe, effective, or may be appropriate for you.
- UPMC disclaims all liability whatsoever for any documentation, information, programs, software, or other material that is or may become a part of our websites or apps. UPMC does not warrant or guarantee that it will be available for your use, that the information will not be offensive to you, or that it will meet your needs and requirements.

Privacy

UPMC is committed to safeguarding your personal information. As described in our Privacy Statement and Notice of Privacy Practices, we keep the personal information of our patients and members in the strictest confidence. UPMC complies with applicable laws, regulations, standards, and guidelines established by governmental agencies and accepted accrediting organizations at all times. These include the European Union's General Data Protection Regulation, where applicable. If you have any questions concerning the confidentiality of your personal information that has been entrusted to UPMC, please contact UPMC's Office of Patient and Consumer Privacy at 412-647-5757, or 1-800-533-UPMC (8762).

Detailed privacy information (including the HIPAA Notice of Privacy Practices) can be found at:

UPMC: <http://www.upmc.com/patients-visitors/privacy-info/Pages/default.aspx>

UPMC Health Plan: <https://www.upmchealthplan.com/privacy.aspx>

Collection and Use of Identifiable Information

We may ask you to provide us with identifiable personal information while using our websites and apps. This information is collected and used only for the purposes indicated where and when the information is requested or collected. If we wish to use your personal information for a new or different purpose, we will offer you the means to consent to this purpose at the point where the use of your personal information is requested. Except as requested by you, or as indicated on the webpage or app where your information is requested, we do not disclose your identifiable personal information to other organizations.

Retargeting, Remarketing, and Re-identification

As you browse **UPMC.com**, advertising cookies will be placed on your computer so that we can understand what you are interested in. Our advertising and marketing partners then enable us to present you with advertising on other sites, or with marketing information, based on your previous interaction with **UPMC.com**.

These advertising partners, as members of the **Network Advertising Initiative ("NAI")**, may have their own privacy policies as well. To remove yourself from some or all NAI member advertising programs, please visit the **NAI Opt-Out Page** and follow the relevant instructions. Please note that if you delete, block, or otherwise restrict cookies on your computer, or if you use a different computer or Internet browser, you may need to renew your NAI opt-out choice.

Data collected by UPMC for advertising or marketing purposes includes information such as the browser type, user location (municipality, not home or street address), IP address, date and time of visit, domain type, and your activity on our website. We also may permit selected marketing partners to match and re-identify you, but only if you have voluntarily provided UPMC with your email address for the receipt of marketing and related information.

What Is Re-identification?

Re-identification is a process by which anonymized data is matched with personally identifiable information. UPMC uses this data in order to provide website visitors with a more relevant and user-friendly online experience.

What Data Is Collected?

Personal data, or personal information, means any information about an individual used to identify that person.

*UPMC does **NOT** collect or re-identify the following information in this process:*

- Protected Health Information (PHI), such as demographic information, medical histories, test and laboratory results, mental health conditions, and insurance information
- Social security numbers
- Information or browsing behavior related to sensitive subjects, including but not limited to sexual health, cancer, substance abuse or disorders, and mental health
- Billing information

How UPMC Uses Your Data

We may use user data to form a picture of what we think you may want or need, or what may be of interest to you. This is how we decide which services and may be relevant for you and tell you about them. We may carry this out across our properties and marketing communications.

How UPMC Protects Your Information

UPMC maintains reasonable standards of security and confidentiality consistent with customary business practices to protect the information under our control from loss, misuse, and alteration.

We also limit access to our website and services by our own employees to the individuals we authorize for the proper handling of such information. Any employee found violating our standards of security and confidentiality will be subject to our disciplinary process. We require that our advertising and marketing partners follow the same policy for their internal staffs.

Can I Opt Out?

Yes. You can control cookies through your browser settings and other tools.

To the extent that a UPMC application requires cookies, restricting cookies may affect ability to use UPMC websites and apps. For example, MyUPMC requires that cookies be enabled on your browser for the website to work as designed. If you choose to block or restrict cookies on your computer, you will not be able to access all the functions and services available through MyUPMC.

Content Review

UPMC's goal is to provide high-quality health information through the content on our websites and apps. We define "content" as all text, images, graphics, tables, audio and video recordings, menu icons, bars, listings, indices, and functions that support content such as links, navigation, searches, and calculations. Every effort has been made to provide accurate and current information that will be useful to the reader.

Much of the information provided on our websites and apps was authored by, or has been reviewed by, UPMC staff. However, some of the consumer education information on our websites and apps is provided through a contract with third parties.

We follow a standard set of editorial procedures for information that we post on our websites and apps. However, we specifically disclaim any guarantees or warranties, whether expressed or implied, as set forth in detail below. It is the responsibility of visitors to our websites to evaluate the information we provide and determine its relevancy and usefulness to them.

UPMC uses original, licensed stock, and purchased photography on our websites and apps. The individuals portrayed in the images may be models, and their inclusion is not intended to imply any endorsement or association with any illness or condition.

Please contact our Webmaster (**webmaster@upmc.edu**) with any feedback or concerns about the content provided on our websites and apps.

User Accounts

You are responsible for the secure and proper use of any user accounts that you establish on our websites and apps. You are also responsible for any actions taken utilizing your user account(s). UPMC strongly encourages you to not share your username and password. You understand that UPMC takes no responsibility for, and disclaims all liability for damages arising from, your sharing your account(s) with others, or your account(s) being compromised. If at any time you feel that your user account has been compromised or that your information has been inappropriately disclosed or used in any way, you should immediately (a) change your password, then (b) contact UPMC. If UPMC has reason to believe that your account has been compromised or misused, UPMC may suspend or discontinue your account(s) without prior notice.

Acceptable Use

You agree not to access or use your account that you create on our website or app in an unlawful way or for an unlawful or illegitimate purpose, or in any manner that is not consistent with these terms. You shall not post, use, store, or transmit (a) a message or information under a false name; (b) information that is knowingly wrong or deceptive, unlawful, libelous, defamatory, obscene, fraudulent, predatory of minors, harassing, threatening, or hateful to any person; or (c) information that infringes or violates any of the intellectual property rights of others or the privacy or publicity rights of others. You shall not attempt to disrupt the operation of our websites or apps by any method, including through the use of viruses, Trojan horses, worms, time bombs, denial of service attacks, flooding, or spamming. You shall not use your account in any manner that could damage, disable, or impair our website or app. You shall not attempt to gain unauthorized access to any user accounts, computer systems, or networks through hacking, password mining, or any other means. You shall not use any robot, scraper, or other similar means to access your account for any purpose.

Social Media

UPMC encourages open dialogue and appreciates the importance of the visitor experience. In certain cases, UPMC may give you the opportunity to post information on one of our websites or other social media sites in which UPMC participates (such as Facebook). We encourage you to share your story, to "like" any post, and to share with your friends using "share" links. Discussions, questions, and commentary are welcome, and UPMC asks that posts be respectful. Through UPMC's participation on any social media site, UPMC agrees to observe the site's posting guidelines and terms of use, as well as our own.

UPMC shall not be held responsible for content submitted by other social media site users. UPMC also reserves the right, but is not obligated, to remove any posts, graphics, comments, videos, photos, or any other content that:

- Is libelous, defamatory, or disparaging
- Violates another party's copyright, trademark, or other intellectual property rights
- Affects the privacy rights of any of our patients, including the person posting the content, or of any UPMC employee
- Condone or promotes illegal activity
- Is inaccurate, misleading, fraudulent, or deceptive
- Uses harsh, obscene, hateful, or threatening language
- Is spam, or is intended to cause technical disruptions to a UPMC website or social media site
- Offers unauthorized advice or tips
- Markets commercial products or solicits monetary contributions to any organization
- Is off-topic or excessive
- Violates any applicable law

UPMC is not obligated to respond to any post or request for information or advice made on a social media site. Any health information provided is for informational purposes only and is not a substitute for professional medical advice.

Online Forms

At times, UPMC may ask you for personal information while you are visiting our website. We ask for this information only to deliver materials that you have requested, to respond to a question you have asked, or to provide you with a product or service.

When you enter data into an online form on our website, the personal information you type is protected and securely transmitted to us through a method such as a Secure Sockets Layer (SSL). SSL is the standard method that websites use to protect visitors' information by coding or "encrypting" everything from credit card transactions to enrollment data.

All of the health information that you provide to us through this website is subject to the protections outlined in our Privacy Statement and Notice of Privacy Practices.

Links to other sites

Throughout UPMC's websites and apps, links may be provided to non-UPMC websites. These links are provided only as a convenience. If you decide to access these linked websites, you do so entirely at your own risk. UPMC has no responsibility or control over the content or security of these websites, and makes no representations and gives no warranties with respect to the accuracy or completeness of any information contained therein. The inclusion of any link does not imply affiliation, endorsement, or adoption by UPMC of the linked website or its content, nor of the organization hosting the website. UPMC asks that you take appropriate precautions to ensure that whatever links you select are free from viruses and other types of malware. You agree that UPMC shall not be responsible for any loss or damage of any kind incurred because of your access or use of these websites.

Children's Privacy

UPMC is committed to protecting the privacy of children. UPMC's websites and apps are not intended or designed to attract children under the age of 13. We do not knowingly collect, maintain, or use personal information from children under 13 years of age, and no part of our websites are directed to children under the age of 13. If you learn that your child has provided us with personal information without your consent, you may alert us at **webmaster@upmc.edu**. If we learn that we have collected any personal information from children under 13 years old, we will promptly take steps to delete such information.

Device Compatibility

UPMC cannot guarantee that every device (smartphone, tablet, or PC) or Internet browser is capable of properly performing all functions of all UPMC websites and apps. If your device does not permit you to perform a website function, you should use a different compatible device instead. UPMC is committed to providing information platforms that are reasonably accessible to all users, including those with disabilities.

Security

UPMC is committed to compliance with all federal, state, and local laws, as well as applicable regulations, standards, and guidelines established by government agencies and accepted accrediting organizations.

While UPMC uses industry-accepted practices and technologies to secure our websites and apps, you should take appropriate precautions to protect personal and confidential information, and to use your devices/apps in a secure and responsible manner. UPMC is not responsible for the security of your devices, and expects that you will configure them in a secure and responsible manner.

We will provide a secure transmission method for you to send us your personal information. While such secure transmission methods provide reasonable protections against unauthorized access, if you have concerns regarding the transmission of sensitive information, you should consider using nonelectronic communication methods.

All UPMC staff and consultants who have access to or are involved with the processing of personal information have been trained to respect the confidentiality of your personal information.

Warranty Disclaimer

Your use of any UPMC website or app (including any associate accounts) is at your sole risk and is provided on an “as is” and “as available” basis. UPMC and its affiliates expressly disclaim all warranties of any kind, whether express or implied, including, but not limited to:

- a. Warranties of merchantability, fitness for a particular purpose, and noninfringement;
- b. Warranties that (i) UPMC’s website(s) and apps will meet your requirements, (ii) UPMC’s website(s) and apps will be uninterrupted, timely, secure, or error-free, (iii) the results that may be obtained from the use of UPMC’s website(s) and apps will be accurate or reliable, (iv) the quality of any products, services, information, or other material purchased or obtained through UPMC’s website(s) or apps will meet your expectations, and (v) any errors associated the UPMC’s website(s) or apps will be corrected;
- c. any inaccuracies or defects in the information, software, communication lines, the Internet or your Internet service provider (ISP), computer hardware or software, or any other service or device that you use to access our websites and apps; and
- d. Warranties regarding advice and information obtained by you through UPMC’s website(s) and apps — except as expressly stated in the terms associated with the website or app.

You shall be solely and fully responsible for any use or disclosure of information caused by you or any person using your username and password. UPMC does not assume any responsibility for any loss, damages, or liabilities arising from the failure of telecommunications infrastructure, the Internet, or your misuse of any protected health information, advice, ideas, information, instructions, or guidelines accessed through UPMC’s website(s) and apps. Should you have reason to believe that your information is not accurate, you should contact UPMC immediately.

Limitation of Liability

Under no circumstances shall UPMC, any UPMC affiliates, or any UPMC licensor or supplier be liable in any way for your use of our website(s) or apps, including, but not limited to, any errors or omissions in any content, any infringement of the intellectual

property rights or other rights of third parties, or for any loss or damage of any kind incurred as a result of the use of such website or app.

To the maximum extent permitted by law, in no event shall UPMC or any of its affiliates be liable for any direct, indirect, special, punitive, indirect, incidental or consequential damages of any kind, including, but not limited to damages resulting from: (i) personal injury, wrongful death, loss of use, loss of profits, interruption of service, or loss of data; or (ii) mistakes, omissions, interruptions, deletion of files, errors, defects, delays in operation or transmission, or any failure of performance, whether or not limited to acts of god, communication failure, theft, destruction or unauthorized access to your records, programs, or services, and whether in any action in warranty, contract, or tort (including but not limited to negligence or breach), or otherwise arising out of or in any way connected with the use of, or the inability to use, your account or any service accessed through your account or any material or information contained in, accessed through, or products purchased on, our websites or apps, even if UPMC (including its affiliates, any UPMC licensor or supplier, any third party that promotes the UPMC website or app or provides a link to the service) is advised of the likelihood or possibility of the same.

You acknowledge and agree that UPMC and its affiliates' aggregate liability to you for any claim of damages, losses, fees, charges, expenses, or liabilities, and in circumstances where the foregoing limitation is finally determined to be unavailable, shall not exceed the fee paid by you for the good or services that gave rise to the claim.

PLAINTIFFS' EXHIBIT 4

Declaration of Richard M. Smith

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED