

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, SS.

SUPERIOR COURT
C.A. No.:

19-1651

John Doe and Jane Doe, individually and)
on behalf of all others similarly situated,)

Plaintiffs,)

v.)

Partners Healthcare System, Inc.;)

The General Hospital Corporation)

d/b/a Massachusetts General Hospital;)

Brigham Health, Inc.;)

Dana-Farber Cancer Institute, Inc.;)

Dana-Farber / Partners Cancer Care, Inc.; and)

Dana-Farber, Inc.)

Defendants.)

SUFFOLK SUPERIOR COURT
CLERK'S OFFICE
2019 MAY 23 P 12:38
MICHAEL JOSEPH DONOVAN
CLERK / MAGISTRATE

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs John Doe and Jane Doe, on behalf of himself and herself and all others similarly situated, bring suit against Defendants Partners Healthcare System, Inc., The General Hospital Corporation doing business as Massachusetts General Hospital, Brigham Health, Inc., Dana-Farber Cancer Institute, Inc., Dana-Farber / Partners Cancer Care, Inc., and Dana-Farber, Inc., and upon personal knowledge as to Plaintiff's own conduct and on information and belief as to all other matters based upon investigation by counsel, alleges as follows:

NATURE OF THE ACTION

1. This case concerns Defendants' systematic violation of the medical privacy rights of their patients.

2. Defendants disclose personally identifiable information about their patients, including their status as patients and the content of patient communications with Defendants, to

Facebook and other third parties without their patients' knowledge or consent.

3. Defendants' conduct in disclosing personally identifiable information about their patients to Facebook and other third parties violates the privacy laws of the Commonwealth of Massachusetts, including but not limited to: G.L. c. 272, § 99 (interception of wire and oral communications); G.L. c. 214, § 1B (right of privacy); G.L. c. 111, § 70E (patients' and residents' rights).

4. Under Massachusetts General Law Chapter 214, § 1B, all persons "have a right against unreasonable, substantial, or serious interference" with their privacy.

5. Medical patients in Massachusetts have a valid interest in preserving the confidentiality of communications with health care providers.

6. Health care providers in Massachusetts owe their patients a duty not to disclose information about their patients without a patient's informed written consent.

7. As described below, Defendants have systematically and repeatedly violated Plaintiff's and other patients' privacy rights.

PARTIES TO THE ACTION

8. Defendant Partners Healthcare System, Inc. ("Partners Healthcare") is a Massachusetts corporation with its principal office at 800 Boylston Street, Suite 1150, Boston, Massachusetts 02199.

9. Defendant Partners Healthcare is a parent company for the following member health care entities in Massachusetts: Massachusetts General Hospital, Brigham and Women's Hospital, Brigham and Women's Faulkner Hospital, Cooley Dickinson Hospital, Martha's Vineyard Hospital, Nantucket Cottage Hospital, Newton-Wellesley Hospital, North Shore Medical Center, Wentworth-Douglas Hospital, and 21 community health centers in Massachusetts.

10. Defendant The General Hospital Corporation d/b/a Massachusetts General Hospital (“Mass General”) is a hospital in Boston, Massachusetts, incorporated in the State of Massachusetts with its principal office at 55 Fruit Street, Boston, Massachusetts 02114.

11. Defendant Brigham Health, Inc. is a Massachusetts corporation with its principal office at 75 Francis Street, Boston, Massachusetts 02115. Brigham Health, Inc. is composed of Brigham and Women’s Hospital (“BWH”) and Brigham and Women’s Faulkner Hospital (“BWF”) (collectively, with Brigham Health, Inc., “Brigham”).

12. Defendants Dana-Farber Cancer Institute, Inc. (“Dana Farber Cancer Institute”), Dana-Farber, Inc., and Dana-Farber / Partners Cancer Care, Inc. (collectively, with Dana-Farber Cancer Institute, “Dana-Farber”) are related Massachusetts corporations with principal offices in Boston, Massachusetts. Dana-Farber Cancer Institute has its principal office at 450 Brookline Avenue in Boston, Massachusetts, 02215. Dana-Farber, Inc. has its principal office at 44 Binney Street, Boston, Massachusetts, 02115. Dana-Farber / Partners Cancer Care, Inc. has its principal office at 44 Binney Street, BP376, Boston, Massachusetts, 02115.

13. Defendant Partners Healthcare maintains a collaboration and partnership with Dana-Farber called Dana-Farber / Partners CancerCare, Inc.

14. Plaintiff John Doe is an individual residing in Berkshire County, Massachusetts and is a patient at Mass General, and thus also a patient of Partners Healthcare.

15. Plaintiff Jane Doe is an individual residing in Suffolk County, Massachusetts and is a patient at Mass General, BWH, and Dana-Farber Cancer Institute, and thus also a patient of Partners Healthcare, Brigham and Dana-Farber.

FACTS APPLICABLE TO ALL COUNTS

16. Plaintiff John Doe is a patient of Partners through Mass General Hospital.

17. Plaintiff Jane Doe is a patient of Partners through Mass General Hospital, Brigham, and the Dana-Farber Cancer Institute.

18. Defendants maintain websites for patients at, among other websites:

- a. www.massgeneral.org
- b. www.brighamandwomens.org, and
- c. www.danafarber.org

19. Defendants' websites are designed for patients to communicate with Defendants, including scheduling appointments, paying bills, signing-up and signing-in to a personal patient portal, and learning more about personal conditions, treatments, doctors, and services.

20. As health care providers, Defendants have fiduciary, common law, and statutory duties to protect the confidentiality of patient information and communications.

21. In addition, Defendants expressly promise patients that Defendants will maintain the confidentiality of patient communications and personally identifiable information.

22. Defendants' patients, including Plaintiffs and Class Members, have reasonable expectations of privacy that their personally identifiable information and communications with Defendants will not be disclosed to third parties by Defendants without their express authorization.

23. Notwithstanding Defendants' legal duty of confidentiality and express promises to the contrary, Defendants disclose and permit third parties to record the contents of patients' communications at www.massgeneral.org, www.brighamandwomens.org, and www.danafarber.org without patients' knowledge or consent.

24.

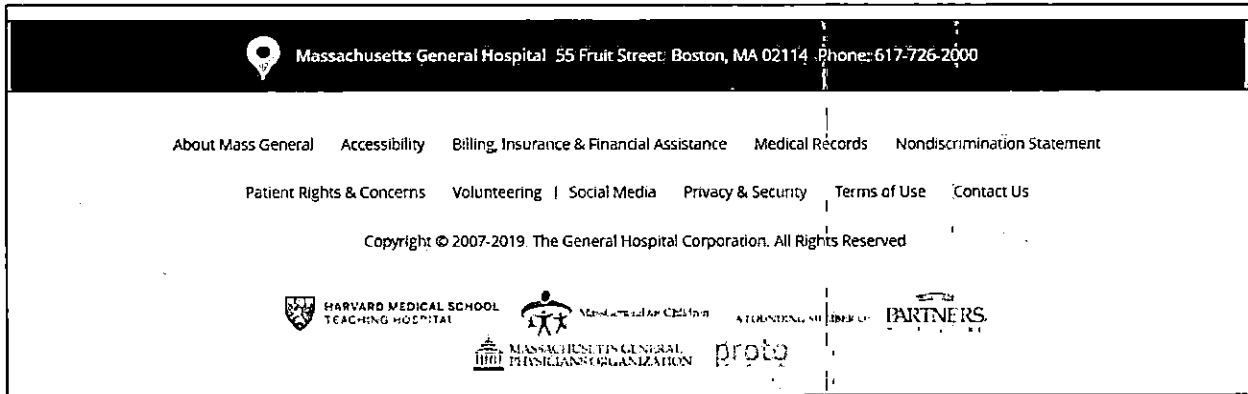
MASS GENERAL HOSPITAL

25. MassGeneral.org is designed for communications with Defendants' patients.
26. As depicted below, the Mass General homepage provides patients with tools to sign-in to the "Patient Gateway," "Find a Doctor," "Request an Appointment" and find more information about their own "Conditions & Treatment" or "Patient & Visitor Info."

The screenshot shows the Mass General Hospital homepage. At the top, there is a navigation bar with links for Patient Gateway, Patient & Visitor Info, For Health Professionals, Careers, News, Giving, and a language selector set to English. Below this is a secondary navigation bar with links for Conditions & Treatments, Centers & Departments, Education & Training, Research, Find a Doctor, Find a Researcher, and Appointments & Referrals. The main content area features a large banner with the headline "Revolutionizing Care" and a sub-headline stating "Mass General is consistently ranked as one of the top hospitals in the nation by U.S. News & World Report." A "LEARN MORE" button is positioned below the text. To the right of the text is a photograph of the hospital building. Below the banner, there is a "GET STARTED" section with a list of services: Find a Doctor, Request an Appointment, Refer a Patient, Partners Patient Gateway, and Locations. To the right of this list is a "Featured Stories" section with two articles: "Share Your Love This February" and "Mass General Plans for New Clinical Facility". Further right is a "Committed to Quality and Safety" section with a bar chart and a building icon.

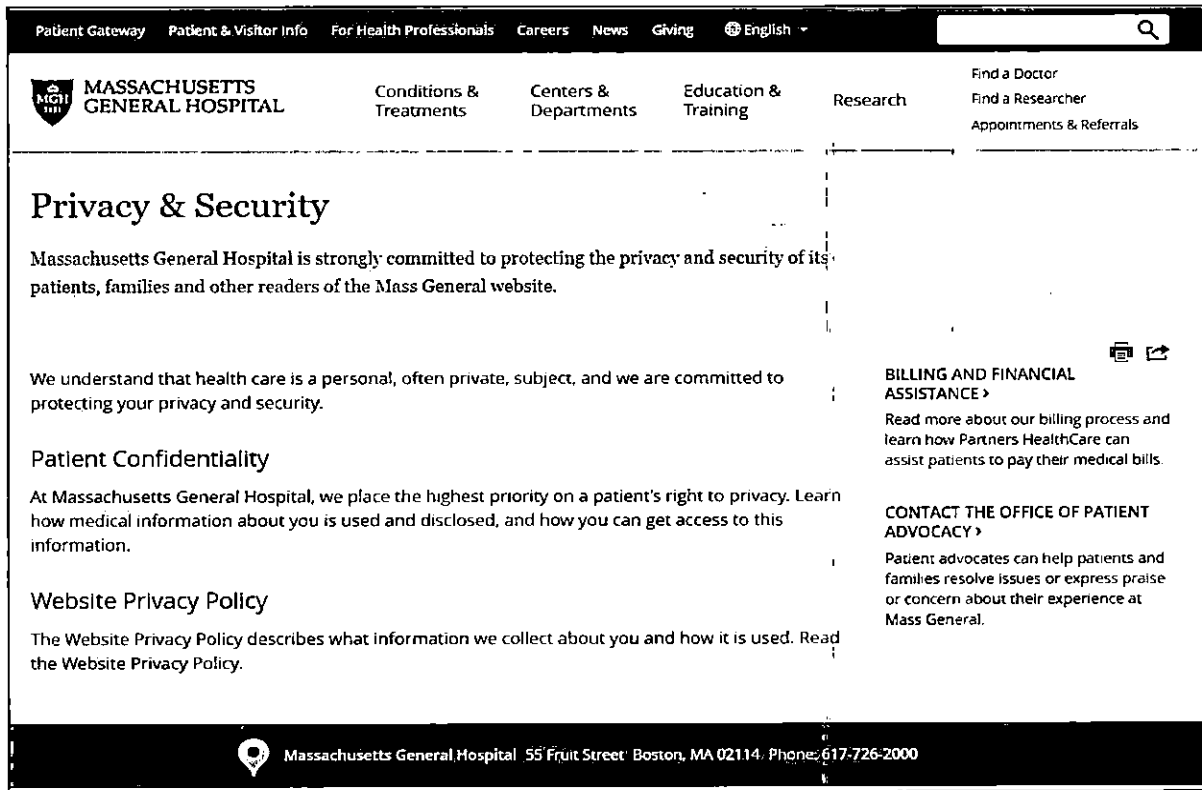
Mass General's Privacy Promises

27. The footer at www.massgeneral.org contains a link to "Privacy & Security."



28. To click on the “Privacy & Security” link, a patient must scroll down to a submerged screen and then find it from a group of 12 separate links in small type.

29. When a patient clicks Privacy & Security, they are taken to the following page:



30. A patient who views this page would reasonably anticipate that the “Patient Confidentiality” link applies to patients.

¹ <https://www.massgeneral.org/notices/privacy/> (last accessed April 30, 2019). **[Update access dates prior to filing]**

31. By clicking on the “Patient Confidentiality,” patients are taken to a page (partially depicted below) containing links to Partners Healthcare’s PDF versions of its HIPAA “Notice for Use of and Sharing of Protected Health Information.” Defendants Partners Healthcare and Mass General expressly promise, “[a]t Massachusetts General Hospital, we place the highest priority on a patient’s right to privacy. We respect the privacy and confidentiality of each patient’s health information.”²

The screenshot shows the top navigation bar of the Massachusetts General Hospital website. The navigation menu includes: Patient Gateway, Patient & Visitor Info, For Health Professionals, Careers, News, Giving, and English. Below the navigation bar is the MGH logo and the text "MASSACHUSETTS GENERAL HOSPITAL". To the right of the logo are links for Conditions & Treatments, Centers & Departments, Education & Training, Research, Find a Doctor, Find a Researcher, and Appointments & Referrals. The main content area is titled "Patient Confidentiality" and contains the following text: "At Massachusetts General Hospital, we place the highest priority on a patient's right to privacy. We respect the privacy and confidentiality of each patient's health information." Below this text is a section titled "Health Insurance Portability and Accountability Act (HIPAA)" which states: "Mass General adheres to the requirements outlined by the Health Insurance Portability and Accountability Act (HIPAA), which ensures security and privacy of an individual's medical records and promotes privacy and trust between patients and their health care providers." It further explains that as part of HIPAA requirements, all new patients seeing their health care provider upon their initial visit are required to sign an acknowledgement form to indicate that they have received the Privacy Notice. The Privacy Notice describes how the hospital/provider uses and shares your personal health information. At the bottom of the page, there are links to view the Partners HealthCare Notice for Use of and Sharing of Protected Health Information for more information about your privacy rights as a patient. Below this are three links for PDF versions: English version PDF, Versión en Español PDF, and Versão em Português PDF. On the right side of the page, there is a dark box with the text "Partners HealthCare Notice for Sharing Information" and links for "Versión en Español (PDF)" and "Versão em Português (PDF)".

² <https://www.massgeneral.org/notices/privacy/patientconfidentiality.aspx> (last accessed April 30, 2019).

32. Upon clicking on the HIPAA PDF link, patients are taken to Partners Healthcare HIPAA Notice of Privacy Practices.³ The Partners Healthcare HIPAA Notice of Privacy Practices advises, among other things, that Mass General “will not share your health information for other purposes not described in this Notice unless you give us your written permission.”⁴ Significantly, the HIPAA Notice of Privacy Practices does not describe any disclosures of patient communications and personally identifiable information to third-party data companies for advertising purposes.⁵

33. Plaintiffs and Class Members did not provide Defendants’ with written permission to disclose their personally identifiable information to third parties as alleged herein.

34. A patient who bypasses the link to “Patient Confidentiality” and instead clicks on the link to the “Website Privacy Policy” is sent to a separate policy.

35. The Mass General Website Privacy Policy gives users the impression that patient personally identifiable information is not disclosed to third parties. The purported Website Privacy Policy begins with the assurance, “Massachusetts General Hospital is committed to protecting the privacy and security of the users of its websites.”⁶

36. Mass General further states, “At Mass General, we are committed to protecting the privacy and security of visitors to our websites. This Privacy Policy will tell you what information we collect, how it is used and your options as you interact with our sites.”⁷

³ Partners Healthcare HIPAA Notice of Privacy Practices obtained via https://www.partners.org/Assets/Documents/Notices/Partners_Privacy_Policy_English.pdf (last accessed April 30, 2019), annexed hereto as Exhibit 1.

⁴ *Id.* at 6.

⁵ *Id.*

⁶ Mass General Website Privacy Policy, obtained via <https://www.massgeneral.org/notices/privacy/websiteprivacy.aspx> (last accessed April 30, 2019), annexed hereto as Exhibit 2.

⁷ *Id.* at 2.

37. The Mass General Website Privacy Policy expressly promises, “Mass General never shares any personal information you provide when requesting information with third parties, except as required by law or in order to provide the services requested.”⁸

38. Mass General does not inform patients, however, that it discloses the content of patient communications and patient personally identifiable information to third-parties, including Facebook.

39. In addition, Mass General’s purported Website Privacy Policy states, “Patients can opt to create a Partners Patient Gateway account. Partners Patient Gateway is a secure portal available for patients to manage their health.”⁹

40. Mass General does not inform patients, however, that creation of a Partners Patient Gateway account causes disclosure of patient status to third parties.

41. Mass General states that it uses “cookies, tracking pixels, and related technologies” in its capacity as a first-party,¹⁰ but fails to disclose that it routinely discloses personally identifiable information about users to third parties, such as Facebook

42. As a matter of law, even if Mass General’s privacy policy expressly stated that it made disclosures of personally identifiable information to third parties, that would not be sufficient evidence of consent because:

a. Disclosure of personally-identifiable information about a patient may only be made pursuant to a lawful HIPAA notice and/or the patient’s express, informed written consent; and,

b. The Policy is not provided in a way that provides patients with

⁸ *Id.* at 4.

⁹ *Id.* at 2.

¹⁰ *Id.* at 3-4.

constructive notice of its terms.

BRIGHAM

43. Brigham maintains BrighamandWomens.org to communicate with patients.

44. As depicted below, the homepage provides patients with tools to sign-in to the “Patient Gateway,” “Find a Doctor,” “Request Appointment” and learn about “Services,” “Insurance, Billing and Payments,” “Clinical Trials,” and “Patient & Visitor Info.”

The screenshot shows the Brigham Health website homepage. At the top left is the Brigham Health logo with the text "BRIGHAM HEALTH" and "BRIGHAM AND WOMEN'S HOSPITAL". To the right of the logo are navigation links: "LOCATIONS", "FIND A DOCTOR", "REQUEST APPOINTMENT", "PATIENT GATEWAY", and "GIVING". There is also a "Select Language" dropdown menu and a search icon. Below the navigation is a dark banner with three categories: "PATIENTS AND FAMILIES", "MEDICAL PROFESSIONALS", and "RESEARCH". The main content area features a large image of a person's hands holding a stethoscope. Below the image is the text "BRIGHAM HEALTH" and "Helping our patients and their families get back to what matters most." followed by a link "ABOUT BWH >". On the left side, there is a section titled "WHAT CAN WE HELP YOU WITH?" with four buttons: "FIND A DOCTOR", "REQUEST APPOINTMENT", "LOCATIONS", and "SERVICES". Below these buttons are links for "Insurance, Billing and Payments", "Directions & Parking", "Patient Gateway", and "Clinical Trials". In the center, there is a graphic with the text "Congratulations to our Brigham Health Top Doctors" and a photo of a doctor. Below this is the heading "BRIGHAM HEALTH PHYSICIANS NAMED 'TOP DOCTORS'" and a paragraph: "More than 275 Brigham Health physicians were included on Boston magazine's 2019 list of 'Top Doctors.' To prepare the annual list, Boston magazine partners with Castle Connolly Medical Ltd., a health care". On the right side, there is a graphic for "BEST HOSPITALS US NEWS HONOR ROLL 2018-19". Below this is the heading "BWH NAMED TO US NEWS & WORLD REPORT'S HONOR ROLL" and a paragraph: "Brigham and Women's Hospital has ranked among the top 20 best hospitals in the nation on US News and World Report's Best Hospitals Honor Roll." followed by a link "LEARN MORE >".

Brigham's Privacy Promises

45. The footer at www.brighamandwomens.org contains two links with the word “Privacy,” with one that expressly applies to patients.



46. The “Patient Privacy Notice” links takes patients to the Partners Healthcare’s HIPAA Notice of Privacy Practices, which, as described above, promises to keep personally identifiable information confidential.¹¹

47. The Partners Healthcare HIPAA Notice of Privacy Practices promises patients, “We will not share your health information for other purposes not described in this Notice unless you give us your written permission.”¹² The Notice does not describe any disclosures of personally identifiable information to third-party data companies for advertising purposes.

48. Plaintiffs and Class Members did not provide Defendants’ with written permission to disclose their personally identifiable information to third parties as alleged herein.

49. Brigham’s separate “Privacy Policy” page fails to disclose that personally identifiable information is routinely disclosed to third-parties. The Privacy Policy page provides information regarding Brigham’s “Website Consent and Privacy Policy.” It begins with the assurance, “At Brigham and Women’s Hospital, we are committed to using all reasonable efforts to protect the privacy and security of the users of our website. We understand that health is a

¹¹ See Partners Healthcare HIPAA Notice of Privacy Practices, Exhibit 1.

¹² *Id.* at 6.

very personal, private subject.”¹³

50. Brigham informs users that it “collect[s] and log[s] the IP address of visitors to brighamandwomens.org,” but assures users, “[t]o maintain your privacy, we do not associate IP addresses with records containing personal health information.”¹⁴

51. Brigham states that it uses cookies, tracking, and Internet-based advertising to help “analyze how users use different resources and help us improve our site. This information may also be used to target related Brigham and Women’s Hospital advertisements to you on other third-party sites. Collecting this information does not allow us to personally identify you.”¹⁵ This omits a material fact: that Brigham uses third-party cookies, tracking, and advertising to disclose personally identifiable information about patients to third parties.

52. Brigham also states that it “may occasionally provide statistics to third parties related to the number of visitors who use the site. These statistics do not provide personally identifiable information.”¹⁶ This omits a material fact: that Brigham uses other methods to disclose personally identifiable information to third parties.

53. As a matter of law, even if Brigham’s privacy policy expressly stated that it made disclosures of personally identifiable information to third parties, that would not be sufficient evidence of consent because:

- a. Disclosure of personally identifiable information about a patient may only be made pursuant to a lawful HIPAA notice and/or the patient’s express, informed written consent; and,

¹³ Brigham’s Website Consent and Privacy Policy, obtained via <https://www.brighamandwomens.org/about-bwh/privacy> (last accessed April 30, 2019), annexed hereto as Exhibit 3.

¹⁴ *Id.* at 1-2.

¹⁵ *Id.* at 3.

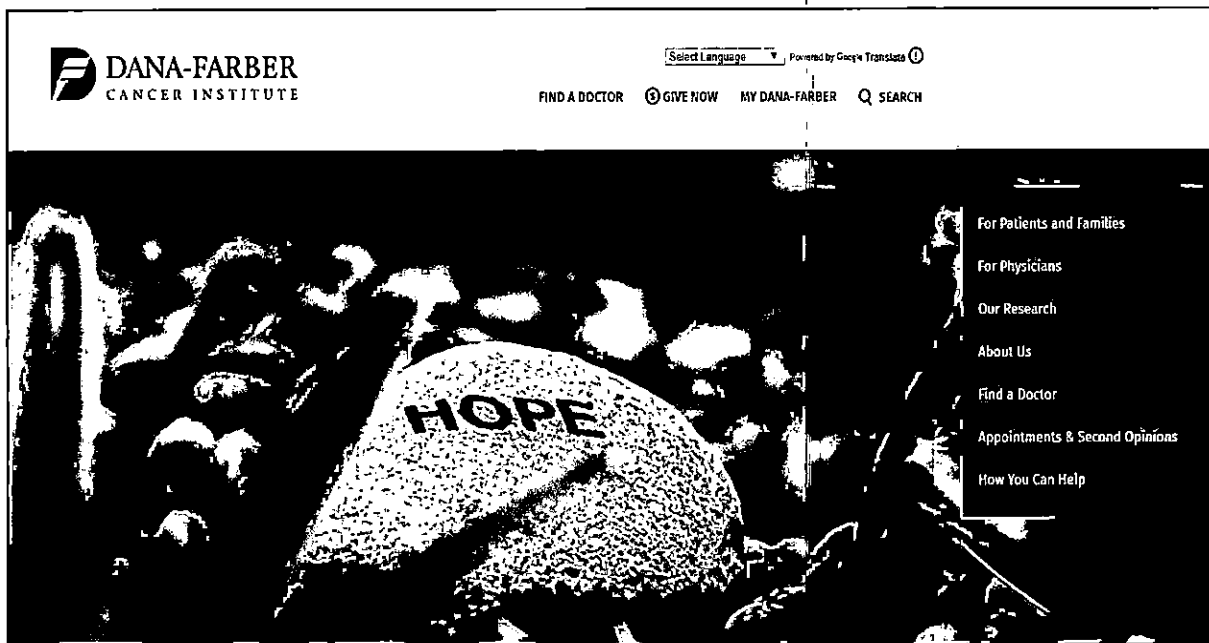
¹⁶ *Id.* at 4.

b. The Policy is not provided in a way that provides patients with constructive notice of its terms.

DANA-FARBER

54. [Dana-Farber.org](https://www.dana-farber.org) is designed for communications with patients.

55. As depicted below, the Dana-Farber homepage provides patients with tools to sign-in to “My Dana-Farber”, Find a Doctor, set up appointments or seek a second opinion, and to obtain information “For Patients and Families.”



Dana-Farber's Privacy Promises

56. Dana-Farber's HIPAA Notice of Privacy Practices promises patients, “we *never* share your information unless you give us written permission” for “Marketing purposes” or the “Sale of your information.”¹⁷

¹⁷ Dana-Farber HIPAA Notice of Privacy Practices, obtained via [https://www.dana-farber.org/uploadedFiles/Pages/For Patients and Families/Becoming a Patient/Practical and Legal Matters/english-notice-of-privacy-practices.pdf](https://www.dana-farber.org/uploadedFiles/Pages/For%20Patients%20and%20Families/Becoming%20a%20Patient/Practical%20and%20Legal%20Matters/english-notice-of-privacy-practices.pdf) (last accessed April 30, 2019), annexed hereto as Exhibit 4.

57. The footer at www.dana-farber.org contains a link to a website Privacy Policy. To view the link, a patient must scroll down through several submerged screens.

58. The Dana-Farber Website Privacy Statements expressly promises not to disclose personally identifiable information about patients or users.¹⁸

59. Dana-Farber promises, “At Dana-Farber, we place the highest priority on privacy and understand that health is a very personal, private subject. We ensure all reasonable efforts are taken to protect the privacy and security of your information.”¹⁹

60. Under “Confidentiality,” Dana-Farber promises, “A user may collect information about Dana-Farber or use our website without disclosing personal, identifying information.”²⁰

61. Under “Privacy and Confidentiality of Your Health Information,” Dana-Farber promises, “The privacy and confidentiality of your health information are very important to us. It is our duty to protect these, as well as your rights regarding your health information.”²¹

Immediately below this promise, Dana-Farber provides patients and users with a link to “Learn more about the privacy and confidentiality of your health information.” Clicking on this link sends a user to the Dana-Farber HIPAA Notice of Privacy Practices (Exhibit 4).

62. Under “Security,” Dana-Farber promises that it “takes every precaution to protect our users’ information.”²²

63. Under “Cookies,” Dana-Farber discloses that it uses first-party cookies, but does not disclose its use of third parties cookies associated with the disclosure of personally identifiable information. It states, “The Dana-Farber website uses cookies to track traffic coming

¹⁸ Dana-Farber Website Privacy Statement, obtained via <https://www.dana-farber.org/privacy-policy/> (last accessed April 30, 2019), annexed hereto as Exhibit 5.

¹⁹ *Id.* at 1.

²⁰ *Id.*

²¹ *Id.*

²² *Id.*

to our site. We do not collect personal data such as name, telephone number, email, or mailing address. Cookies will also be used to identify a person who chooses to register on our site. If you choose to register on our site and are given a password, choose to give gifts online, or choose to enroll in our email subscription services, we will identify you with cookies. You will always have the opportunity to opt out at any time.”²³

64. Under “Information Collection and Use,” Dana-Farber promises, “Dana-Farber is the sole owner of personal, protected health and donor information collected on this site. We will not sell, share, or rent personal medical information to others.”²⁴

65. As a matter of law, even if Dana-Farber’s privacy policy expressly stated that it made disclosures of personally identifiable information to third parties, that would not be sufficient evidence of consent because:

a. Disclosure of personally-identifiable information about a patient may only be made pursuant to a lawful HIPAA notice and/or the patient’s express, informed written consent; and,

b. The Policy is not provided in a way that provides patients with constructive notice of its terms.

DEFENDANTS’ VIOLATIONS OF THEIR PRIVACY PROMISES & CONFIDENTIALITY OBLIGATIONS TO PATIENTS

66. Defendants disclose Plaintiffs’ and Class Members’ PII, including their status as patients and the contents of their communications with Defendants, to the following third-parties:

a. At www.massgeneral.org, Defendants cause disclosures to Facebook,

²³ *Id.* at 2.

²⁴ *Id.*

Google, LinkedIn, AddThis, Marketo, and SiteImprove.

b. At www.brighamandwomens.org, Defendants cause disclosures to Facebook, Google, and Marketo.

c. At www.dana-farber.org, Defendants cause disclosures to Facebook, Google, AbTasty, and Hotjar.

67. Defendants unauthorized disclosures to third parties includes information that identifies Plaintiffs and Class Members as patients and aids the third-parties in receiving and recording patient communications pertaining to or about specific doctors, conditions, treatments, payments, and connections to the Patient Portal.

68. In making such disclosures, Defendants acted contrary to their promises, legal duties, and Plaintiffs' and Class Members' reasonable expectations of privacy.

**THE NATURE OF DEFENDANTS' INTENTIONAL, UNAUTHORIZED,
UNNECESSARY, AND UNLAWFUL DISCLOSURES**

69. Defendants' third-party disclosures occur because Defendants intentionally deploy source code at www.massgeneral.org, www.brighamandwomens.org, and www.danafarber.org that commandeers patients' web-browsers and causes personally identifiable information, as well as the exact contents of communications exchanged between Defendants and their patients, to be sent to third parties.

70. Defendants' third-party disclosures occur contemporaneous to communications with Plaintiff and Class Members.

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

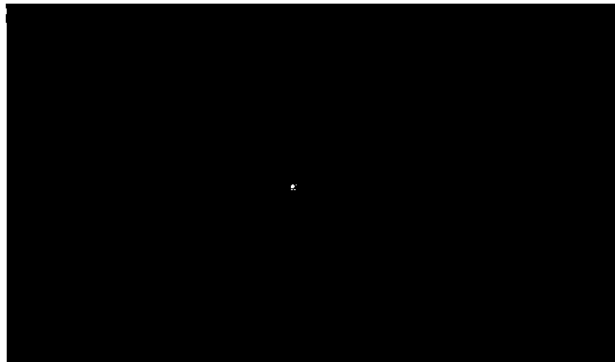
72. Defendants are not required to make disclosures to Facebook, Google, AbTasty, AddThis, Hotjar, Marketo, or SiteImprove for the websites or services to function.

73. These third-party disclosures are made by Defendants without the patients' knowledge, consent, or any affirmative action taken by the patients.

74. In effect, Defendants provide these third-parties with a secret and invisible "window" through which to spy on patient communications and gain PII about the patients.

The Tracking Pixel

75. At Mass General, Brigham, and Dana Farber, disclosures are made through an invisible tracking pixel: a one-by-one pixel (the smallest dot on the user's screen) that is purposefully camouflaged to be the same color as surrounding pixels. An example of a pixel surrounded by a contrasting background can be seen below.



An example pixel – depicted as the white dot in the middle of the image above – can be viewed at <https://www.facebook.com/tr>.

76. In this case, Defendants cause disclosures of patients' personally identifiable information and communications to be sent to Facebook through an invisible tracking pixel.

Google Tag Manager

77. Defendants utilize Google Tag Manager, which provides web-developers with a short-cut to replace the source code from dozens of websites with a short source code from

Google.²⁵

78. Google Tag Manager acts as a Trojan horse, causing disclosures to Google and any other third-party that the web-developer chooses to place within the Google Tag Manager.²⁶

79. The Google Tag Manager source code deployed by Defendants at Mass General, Brigham, and Dana Farber is invisible to patients.

80. The Google Tag Manager Source code at Dana Farber provides:

```
49 <!-- Google Tag Manager (noscript) -->
50 <noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-KL4RMT" height="0" width="0"
style="display:none;visibility:hidden"></iframe></noscript>
51 <!-- End Google Tag Manager (noscript) -->
```

81. This Google Tag Manager source code instructs a patient's browser to include an invisible "iframe" within the Dana-Farber website that has a height of "0", a width of "0", "none" as the value for its display, and "hidden" as the value for its visibility.

82. Substantially similar source code from Google Tag Manager appears at Mass General and Brigham.

83. As used at Dana Farber, Mass General, and Brigham, Google Tag Manager creates an invisible window through which multiple third parties are permitted to spy on patients and record patient communications.

84. For example, the Facebook Tracking Pixel source code at Mass General, Brigham and Women's, and Dana Farber is secretly funneled through Google Tag Manager.

85. Defendants then cause disclosures to Facebook through an invisible Facebook

²⁵ Google Analytics, Introduction to Google Tag Manager, YouTube, <https://www.youtube.com/watch?v=KRvbFpeZ11Y> (last accessed April 30, 2019).

²⁶ Measureschool, Facebook Pixel Custom Event Tracking with GTM Part 2, YouTube, <https://www.youtube.com/watch?v=EwBV0MNcQM8> (last accessed April 30, 2019).

Tracking Pixel that renders on the webpage through the invisible Google Tag Manager iframe.

Unauthorized Disclosures Abound Due to Defendants' Conduct

86. Whether accomplished through an inactive logo, third-party tracking pixel, and/or the Google Tag Manager, Defendants command patients' web-browsers to re-direct the precise contents of the patient's personally identifiable information and communications with Defendants to multiple third parties.

87. With each redirected communication, third-party receives some or all of the following:

a. The exact contents of the communication that the patient caused to be sent to Defendants. For example, when a patient searches for "colon cancer treatment" at Mass General, Defendants disclose the following data to third-parties: "/search/q=colon+cancer+treatment."

b. Defendants also disclose personally-identifiable data elements about the patient, including Internet cookies,²⁷ the patient's IP address,²⁸

²⁷ The Federal Trade Commission describes an Internet cookie as follows: "A cookie is information saved by your web browser. When you visit a website, the site may place a cookie on your web browser so it can recognize your device in the future. If you return to that site later on, it can read that cookie to remember you from your last visit and keep track of you over time." Federal Trade Commission, Internet Cookies, <https://www.ftc.gov/site-information/privacy-policy/internet-cookies> (last accessed April 30, 2019).

²⁸ "An IP address, short for Internet Protocol address, is an identifying number for a piece of network hardware. Having an IP address allows a device to communicate with other devices over an IP-based network like the internet. An IP address provides an identity to a networked device. Similar to a home or business address supplying that specific physical location with an identifiable address, devices on a network are differentiated from one another through IP addresses." Tim Fisher, Lifewire.com, What Is An IP Address?, <https://www.lifewire.com/what-is-an-ip-address-2625920> (last accessed April 30, 2019)

unique device identifiers,²⁹ and a browser-fingerprint,³⁰ all of which connect the contents of the communication to the patient.

Cookie Synching with Facebook at Mass General

88. Based on an Internet security policy known as same-origin policy, Web browsers prevent different entities from accessing each other's cookies. For example, Google is prevented from obtaining Facebook cookies in the HTTP headers of an HTTP request.

89. However, Javascript code running in a Web page can bypass the same-origin policy to send a 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." The technique allows cooperating Web sites to learn each other's cookie identification numbers for the same user. Once the cookie synching operating is completed, the two Web sites can exchange information that they have collected and hold about a user (or patient in the case of a hospital). The technique can also be used to track a patient if third-party cookies are being blocked by a browser.

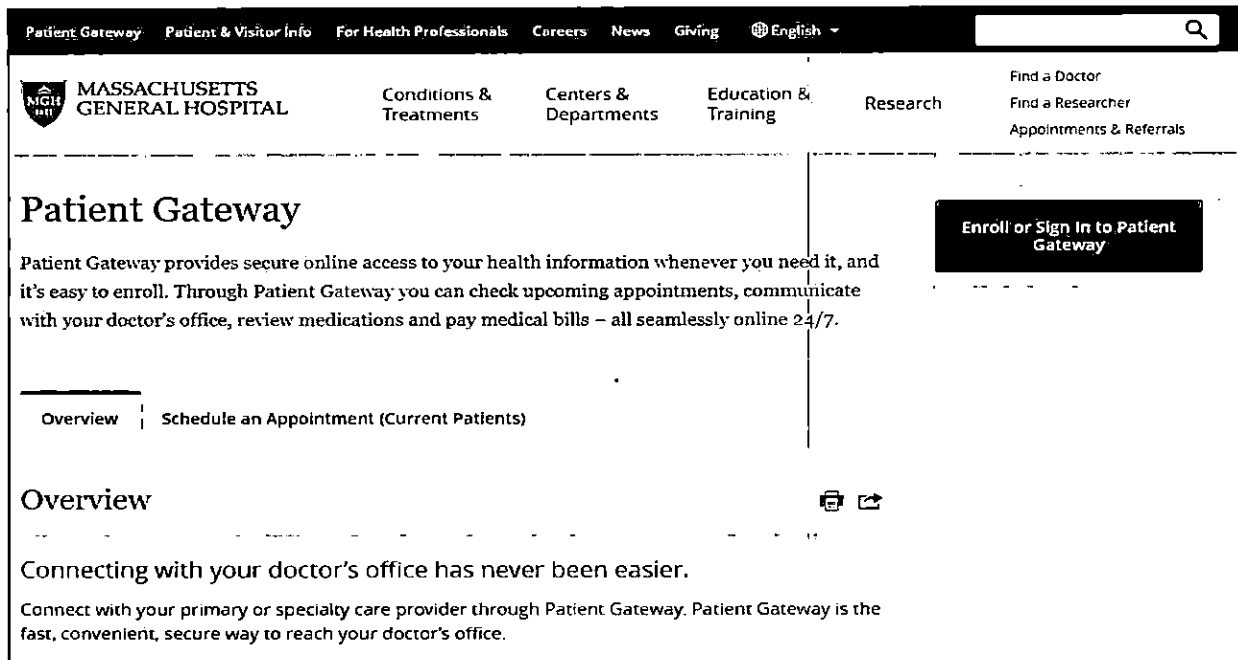
²⁹ "A unique device identifier (UDID) is a unique serial number assigned to each Apple manufactured device. UDID enables the identification, tracking and recording of Apple's suite of iDevices. UDID has many applications, the most important being the ability to identify each device and segregate users according to their demographics, activity within the App Store, etc." Techopedia, Unique Device Identifier, <https://www.techopedia.com/definition/29033/unique-device-identifier-udid> (last accessed April 30, 2019).

³⁰ The Electronic Frontier Foundation explains what a browser fingerprint is as follows: "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 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 build an advertising profile of them." 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> (last accessed April 30, 2019).

90. Cookie synching is used by Defendants at Mass General, Brigham, and Dana-Farber. For example, Mass General, Brigham, and Dana-Farber all set a first-party cookie on patient browsers called “_fbp” which appears to contain a unique identification number with a value identical to that which is disclosed to Facebook in subsequent re-directions of patient communications to Facebook via the Facebook tracking pixel.

Patient Gateway Disclosures by Mass General

91. At Mass General, patients register or log-in to the Patient Gateway by clicking on the green button set forth below:



92. When a patient clicks the “Enroll or Sign In to Patient Gateway” link, Defendants disclose the patient’s personally-identifiable information and the following data to Facebook:

QueryString	
Name	Value
id	[REDACTED]
ev	SubscribedButtonClick
dl	https://www.massgeneral.org/services/patientgateway.aspx
rl	https://www.massgeneral.org/default.aspx
if	false
ts	[REDACTED]
cd[buttonFeatures]	{*classList*: button block -green -large*, *destination*: http://www.patientgateway.org/*, *id*: "", *imageUri* or Sign In to Patient
cd[buttonText]	Enroll or Sign In to Patient Gateway
cd[formFeatures]	[]
cd[pageFeatures]	{*title*: "Patient Gateway - Massachusetts General Hospital, Boston, MA"}

93. Mass General also makes disclosures to Google and AddThis about patient communications on the Patient Gateway page.

Patient Portal Disclosures at Brigham

94. At Brigham, patients can access the Patient Gateway by clicking on links present on every page:

The screenshot shows the Brigham Health website homepage. At the top left is the logo for Brigham Health, Brigham and Women's Hospital. To the right are navigation links: LOCATIONS | FIND A DOCTOR | REQUEST APPOINTMENT | PATIENT GATEWAY | GIVING, followed by a language selection dropdown and a search icon. Below the header is a navigation bar with three categories: PATIENTS AND FAMILIES, MEDICAL PROFESSIONALS, and RESEARCH. The main content area features a large image of medical professionals. Below the image is the text: BRIGHAM HEALTH, Helping our patients and their families get back to what matters most., and ABOUT BWH >. On the left side, there is a section titled 'WHAT CAN WE HELP YOU WITH?' with four buttons: FIND A DOCTOR, REQUEST APPOINTMENT, LOCATIONS, and SERVICES. Below these buttons are links for Insurance, Billing and Payments; Directions & Parking; Patient Gateway; Clinical Trials; International Patients; and Careers. In the center, there is a promotional banner for 'BRIGHAM HEALTH PHYSICIANS NAMED 'TOP DOCTORS'' with a 'VIEW THE LIST >' link. On the right, there is a banner for 'BEST HOSPITALS US NEWS HONOR ROLL 2018-19' with the text 'BWH NAMED TO US NEWS & WORLD REPORT'S HONOR ROLL' and a 'LEARN MORE >' link.

95. When a patient clicks a link to the “Patient Gateway”, Defendants make disclosures to Marketo and Google.

Patient Portal Disclosures at Dana-Farber

96. At Dana Farber, patients register or log-in by clicking on **MY DANA-FARBER**

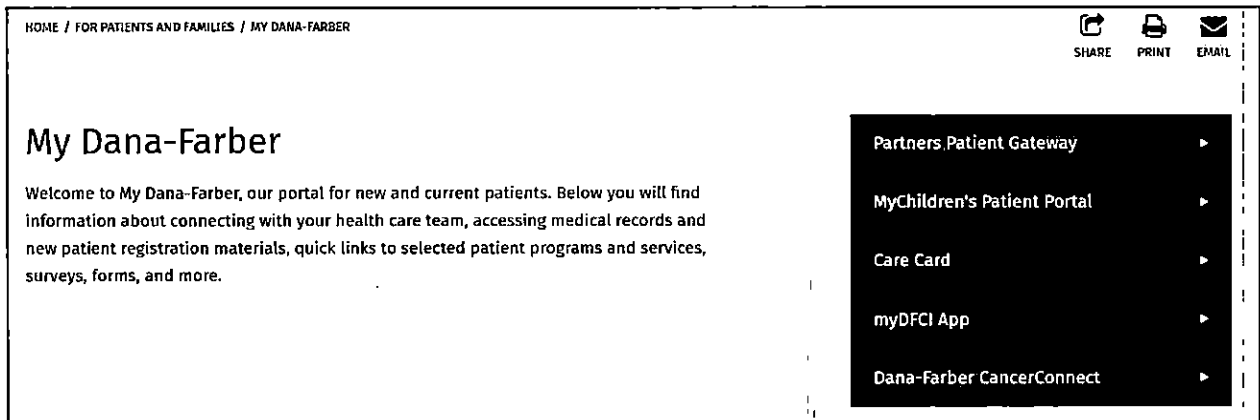


97. When a patient clicks on the My Dana-Farber link, Defendants cause the disclosure of the patient’s personally-identifiable information and the following data to Facebook:

Name	Value
id	[REDACTED]
ev	ViewContent
dt	https://www.dana-farber.org/for-patients-and-families/my-dana-farber/
rl	https://www.dana-farber.org/

98. Defendants also make disclosures of personally-identifiable information and the fact that the patient is viewing the “for-patients-and-families/my-dana-farber” communication to AbTasty, HotJar, and Google.

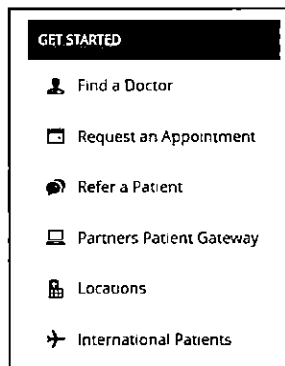
99. These disclosures occur when a patient is at a page with the following:



100. When a patient clicks any of the links in the red column on the right to send further communications to Dana-Farber, the precise contents of those patient communications are also disclosed to Facebook, Google, AbTasty, and Hotjar.

Appointment Disclosures at Mass General

101. At Mass General, patients can request an appointment by clicking on a link:



102. When a patient requests an appointment at Mass General, Defendants cause disclosures of personally-identifiable information and the patient's request to Facebook, Google, AddThis, SiteImprove, and Marketo.

103. The next communication the patient sees from Mass General after sending a “Request an Appointment” communication appears as follows:

Appointments & Referrals
Request an appointment or second opinion, refer a patient, find a doctor or view test results with Massachusetts General Hospital's secure online services.

Get Started | **New Patients** | Existing Patients | International Patients | Referring Providers

New Patients
If you have not previously seen a doctor within the Partners HealthCare Network.

Existing Patients
If you have previously seen a doctor within the Partners HealthCare Network.

For Referring Providers
Refer patients to Mass General by phone or online.

BILLING AND FINANCIAL ASSISTANCE
Read more about our billing process and learn how Partners HealthCare can assist patients to pay their medical bills.

EXECUTIVE HEALTH SERVICES
Learn about our thorough, personalized health evaluation designed to provide comprehensive insights that encourage you to be proactive in managing your health.

104. Regardless of the next communication the patient sends to Mass General, the contents will again be disclosed to Facebook, Google, AddThis, SiteImprove, and Marketo.

105. For those who identify as “new patients,” Mass General sends the following data attached to personally-identifiable information to Facebook, Google, AddThis, SiteImprove, and Marketo: “appointments” and “display=new-patients.”

106. New patients are given additional options to set up an appointment:

Option 1: Contact a Doctor

Search Mass General doctors and request an appointment with the provider of your choice.

Find a Provider

Option 2: Let Us Help You

We offer assistance to patients who would like help choosing a doctor or making an appointment.

To speak with a member of our patient care team, call 800-711-4644 (Monday-Friday 8:30 am-5:00 pm).

You may also submit an appointment request form online.

Request an Appointment

107. Defendants further disclose which option the new patient chooses.

108. When a patient chooses to Request an Appointment, Defendants disclose personally identifiable information and the following data to Facebook:

Name	Value
id	[REDACTED]
ev	SubscribedButtonClick
dl	https://www.massgeneral.org/appointments/default.aspx?display=new-p
rl	https://www.massgeneral.org/appointments/?display=get-started
if	false
ts	[REDACTED]
cd[buttonFeatures]	{"classList":"button -green -thin hasGAEvent","destination":"https://www.massgeneral.org/appointments/an-Appointment","name":"","numChildButtons":0,"tag":"a"}
cd[buttonText]	Request an Appointment
cd[formFeatures]	{}
cd[pageFeatures]	{"title":"Appointments & Referrals - Massachusetts General Hospital, Boston, MA"}

109. Defendants also disclose personally identifiable information and the fact that the

new patient has requested an appointment to Google, AddThis, SiteImprove, and Marketo.

110. Defendants then ask new patients to fill out a form that includes their name, birthdate, address, whether they are the patient, whether they have been referred by a physician, the name of their insurance plan, the best day to call, their medical record number, and any additional details the patient wants to add. At the bottom of the form, Mass General provides a button for the patient to Submit the data:

Best day(s) to call *
 No Preference Monday Tuesday Wednesday Thursday Friday

Address line 1 *

Address line 2

City *

State *

Zip code *

To facilitate processing, please provide insurance plan name if known

About Your Appointment

Have you been referred by a physician? *
 Yes No

Please provide additional details about your request, including the type of specialist, if applicable *

200 character limit

Submit

111. When a patient clicks the “Submit” button, Defendants cause disclosures to

Facebook, AddThis, Google, SiteImprove, and Marketo that the patient has submitted the request with the following data “appointments/appointment-thankyou.aspx” attached to personally-identifiable information about the patient.

112. Facebook source code is capable of scraping the content of form fields. The Facebook source code employed by Mass General includes functions with the following names: “extract PIIFields” and “shouldExtractPIIFromForm.” However, because the Facebook source code has been obfuscated, Plaintiff is without knowledge whether Mass General and Partners have actually implemented form-scraping functionality. Regardless, the names strongly suggests that this capability is employed at Mass General to make disclosures to Facebook.

113. For those who identify as “existing patients” after clicking the “Request an Appointment” button, Mass General sends the following data attached to personally-identifiable information to Facebook, Google, AddThis, SiteImprove, and Marketo: “appointments” and “display=existing-patients.”

114. Existing patients are then provided options:

The screenshot shows a navigation menu with the following items: Get Started, New Patients, Existing Patients (selected), International Patients, and Referring Providers. Below the menu, there are three main sections:

- Contact Your Health Care Provider or Access Center Directly**: To request an appointment with a Mass General doctor, contact that doctor directly. Search Mass General doctors or view all centers and departments for help finding your doctor's contact information.
- Use Patient Gateway**: If your health care provider uses Partners Patient Gateway, you may request an appointment online. **Sign in to Patient Gateway**
- BILLING AND FINANCIAL ASSISTANCE >**: Read more about our billing process and learn how Partners HealthCare can assist patients to pay their medical bills.
- EXECUTIVE HEALTH SERVICES >**: Learn about our thorough, personalized health evaluation designed to provide comprehensive insights that encourage you to be proactive in managing your health.

115. Defendants disclose the patient's choice to Facebook, Google, AddThis, SiteImprove, and Marketo. If the patient chooses to "Sign In to Patient Gateway," Defendants cause a disclosure to Facebook of the following:


QueryString	
Name	Value
id	[REDACTED]
ev	SubscribedButtonClick
dl	https://www.massgeneral.org/appointments/default.aspx?display=existing-patients
rl	https://www.massgeneral.org/appointments/?display=get-started
f	false
ts	[REDACTED]
cd[buttonFeatures]	{ "classList": "button -green -thin hasGAEvent", "destination": "http://www.patientgateway.org/", "id": "", "imageUrl": null, "in to Patient Gateway", "name": "", "numChildButtons": 0, "tag": "a" }
cd[buttonText]	Sign in to Patient Gateway
cd[formFeatures]	[REDACTED]
cd[pageFeatures]	{ "title": "Appointments & Referrals - Massachusetts General Hospital, Boston, MA" }

Appointment Disclosures at Brigham

116. Every page at Brigham provides existing or new patients with prominent links to Request an Appointment:

The screenshot shows the Brigham Health website homepage. At the top, there is a navigation bar with the Brigham Health logo and links for Locations, Find a Doctor, Request Appointment, Patient Gateway, and Giving. Below this is a secondary navigation bar with categories: Patients and Families, Medical Professionals, and Research. A large banner image shows a medical professional interacting with a patient. Below the banner, the text reads "BRIGHAM HEALTH Helping our patients and their families get back to what matters most." Underneath, there are three main content blocks: "WHAT CAN WE HELP YOU WITH?" with buttons for "FIND A DOCTOR", "REQUEST APPOINTMENT", "LOCATIONS", and "SERVICES"; "CONGRATULATIONS TO OUR BRIGHAM HEALTH TOP DOCTORS" with a graphic of a stethoscope and a "TOP DOCTOR" award; and "BEST HOSPITALS US NEWS HONOR ROLL 2018-19" with a graphic of the award. At the bottom, there are links for Insurance, Billing and Payments, Directions & Parking, and Patient Gateway.

117. When a patient requests an appointment, Defendants disclose that fact to Facebook, Google, and Marketo.

118. After a patient clicks Request Appointment, Defendants request their name, gender, address, and the department with which they seek an appointment. At the bottom of the form, they can click the following button: 

119. When a patient clicks the “Request Appointment” button, that fact is disclosed to Facebook in connection with personally-identifiable information about the patient:

Body	
Name	Value
id	[REDACTED]
ev	SubscribedButtonClick
dl	https://www.brighamandwomens.org/forms/request-an-appointment?utm_content=
rl	https://www.brighamandwomens.org/
if	false
ts	[REDACTED]
cd[buttonFeatures]	{“classList”:“”,“destination”:“”,“id”:“”,“imageUri”:null,“innerText”:“”,“name”:“”,“numC
cd[buttonText]	Request Appointment
cd[formFeatures]	[{“id”:“fname”,“name”:“fname”,“tag”:“input”,“inputType”:“text”},{“id”:“lname”,“name
cd[pageFeatures]	{“title”:“Request an Appointment - Brigham and Women’s Hospital”}

Disclosures of Search Queries and Responses

120. When a patient types a search query into a search box at Mass General, Brigham, or Dana-Farber, seeking information about a physician, treatment, or condition, Defendants disclose to third-parties the precise contents of the patient query. For example:

a. At Mass General, when a patient searches for “colon cancer treatment,” Defendants send the precise search term combined with other personally identifiable information to Facebook, AddThis, Google, SiteImprove, and Marketo. The disclosure to Facebook consists of informing Facebook that the patient has engaged in the event of a “Subscribed Button Click,” that the content of the button clicked is “Search,” and that the content of the patient’s search is “q=colon+cancer+treatment.”

b. At Brigham, when a patient searches for “colon cancer treatment,”

Defendants send the precise search term combined with other personally identifiable information to Facebook, Google, and Marketo. The disclosure to Facebook consists of informing Facebook that the patient has engaged in the event of a “Subscribed Button Click,” that the content of the button clicked is “Search,” and that the content of the patient’s search is “text=colon%20cancer%20treatment.”

c. At Dana-Farber, when a patient searches for “colon cancer treatment,” Defendants send the precise search term combined with other personally identifiable information to Facebook, AbTasty, Google, and HotJar. The disclosure to Facebook consists of informing Facebook that the patient has engaged in the event of a “Subscribed Button Click,” that the content of the button clicked is “Search,” and that the content of the patient’s search is “?searchTerm=colon%20cancer%20treatment.”

Disclosures of Providers, Treatments, Conditions, and Bill Payment Information

121. Similar disclosures occur with every communication exchanged between patients and Defendants at Mass General, Brigham, and Dana Farber, including communications about providers, treatments, conditions, and bill payment.

Third-Party Disclosures are Not Necessary

122. None of these disclosures are necessary for health care providers to maintain a website or utilize social media marketing tools.

123. It is possible for a health care website to provide a patient portal without making any disclosures about patient sign-ups or log-ins to third-parties.

124. It is possible for a website developer to enable social media sharing by users without making any automatic disclosures to third-parties.

125. It is possible for a website developer to utilize third-party tracker tools that would identify the parties to communications but obscure the actual contents of the communications

exchanged between the parties.

126. Despite these possibilities, Defendants willfully chose to disclose personally identifiable information about patients and the content of communications exchanged with patients to third-parties.

127. There is no information anywhere at Mass General, Brigham, or Dana Farber to alert patients that their personally identifiable information and the precise contents of their communications (including patient log-ins and communications relating to appointments, medical providers, and specific medical conditions) are disclosed to third-parties contemporaneous to every communication patients exchange with Defendants.

DETAILS ON THE THIRD-PARTIES WHO RECEIVE DEFENDANTS' UNAUTHORIZED, UNLAWFUL DISCLOSURES

Facebook

128. Defendants make disclosures to Facebook via the Facebook Tracking Pixel.

129. Facebook expressly informs developers that the Facebook Tracking Pixel used by Defendants discloses personally-identifiable information to Facebook.

130. The Facebook Tracking Pixel implementation help page for developers informs developers that:

“The Facebook pixel is a snippet of JavaScript code that loads a small library of functions you can use to track Facebook ad-driven 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.”³¹

³¹ Facebook for Developers, Facebook Pixel Implementation Page, obtained via <https://developers.facebook.com/docs/facebook-pixel/implementation/> (last accessed April 30, 2019), annexed hereto as Exhibit 6.

Google

131. Defendants make disclosures to Google via cookies set for advertising purposes at the Google.com domain and the Google advertising subsidiary Doubleclick.com domain.

132. Like Facebook, Google's tracking mechanisms are such that using Google.com or Doubleclick.com (a Google subsidiary) source code on a website will result in the disclosure of PII to Google, including disclosures that occur through the Doubleclick.com domain.³²

AddThis – Oracle

133. Defendants make disclosures to AddThis through the www.addthis.com domain.

134. AddThis is wholly owned by Oracle.

135. The AddThis privacy policy provides as follows:

a. "In our AddThis Terms of Service with the publisher, we require that the publisher informs you directly of how it collects and uses your personal information in this context, and gets your consent where appropriate. Oracle may then also receive information about you via your interactions with the publisher's AddThis Tools, so this Privacy Policy informs you how we process that personal information."³³

b. "AddThis Data is collected online and may indirectly identify you. It includes, for example:

- unique IDs such as a cookie ID on your browser;
- IP addresses and information derived from IP addresses, such as geographic information;

³² Julia Angwin, [Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking](https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking), ProPublica (Oct. 21, 2016, 8 a.m. EDT), <https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking> (last accessed April 30, 2019).

³³ AddThis Privacy Policy, obtained via <https://www.oracle.com/legal/privacy/addthis-privacy-policy.html> (last accessed April 30, 2019), annexed hereto as Exhibit 7.

- information about your device, such as browser, device, type, operating system, the presence or use of ‘apps,’ screen resolution, or the preferred language;
- the date and time you visited a Publisher Site or you used the AddThis Toolbar;
- the referring URL and the web search you used to locate and navigate to a Publisher site[.]”³⁴

c. “We may associate personal information about you with interest segments or profiles as part of the provision of AddThis services to our customers and partners.”³⁵

d. “We use personal information for the following purposes:

- a) To enable AddThis Tools and AddThis Toolbar functionality;
- b) To enable AddThis Publishers and Oracle Marketing & Data Cloud customers and partners to market products and services to you;
- c) To provide personalized recommendations and messages;
- d) To link browsers and apps across devices;
- e) To sync unique identifiers[.]”³⁶

e. “We may share AddThis Data with the following third parties:

- Oracle Marketing and Data Cloud customers and partners, including digital marketers, ad agencies, web publishers, demand side platforms, data management platforms, supply-side platforms, and social media networks.”³⁷

³⁴ *Id.* at 4.

³⁵ *Id.*

³⁶ *Id.*

³⁷ *Id.* at 8.

Marketo

136. Defendants make disclosures to Marketo through the mktosp.com domain.

137. Marketo is a division of Adobe.

138. Marketo's Privacy Policy states that it collects "Personal Data," which it defines as "information that directly, or indirectly identifies you or another individual and which may include: name, title, company name, job function, expertise, postal address, telephone number, email address, browser and device information (including IP address), and information collected through cookies and other similar technologies."³⁸

139. Marketo also states it collects and combines Personal Data online and offline and that it may share such personal data with undisclosed business partners.

AB Tasty

140. Defendants make disclosures to AB Tasty through the abtasty.com domain.

141. AB Tasty states that it collects two types of personally identifiable data: cookies and IP addresses.³⁹

HotJar

142. Defendants make disclosures to HotJar via the hotjar.com domain.

143. HotJar describes itself as "a new powerful tool that reveals the online behavior and voice of" a website's users.⁴⁰ It permits web developers to record patterns of activity by users on a website or particular webpage.

144. Hotjar claims to be more protective of user privacy than the other third-parties to

³⁸ Marketo's Privacy Policy, obtained via <https://documents.marketo.com/legal/privacy/> (last accessed April 30, 2019), annexed hereto as Exhibit 8.

³⁹ AB Tasty's Terms of Use, obtained via <https://www.abtasty.com/terms-of-use/> (last accessed April 30, 2019), annexed hereto as Exhibit 9.

⁴⁰ <https://help.hotjar.com/hc/en-us/articles/115009334567-What-is-Hotjar-> (last accessed April 30, 2019).

whom Defendants make disclosures.

145. HotJar claims to assign each visitor a unique user id so Hotjar can “keep track of returning visitors without relying on any personal information, such as the IP address.”⁴¹

146. HotJar claims, “IP addresses of visitors are always suppressed before being stored ... to ensure the full IP address is never written to disk.”⁴²

147. Hotjar also claims to “automatically suppress[] keystroke data on all input fields” so that it never reaches Hotjar servers.⁴³

SiteImprove

148. Defendants make disclosures to SiteImprove via the siteimprove.com domain.

149. SiteImprove is a digital marketing company.

150. 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.”⁴⁴

⁴¹ Hotjar’s Data Safety, Privacy & Security, obtained via <https://help.hotjar.com/hc/en-us/sections/115003180467-Privacy-Security-and-Operations> (last accessed April 30, 2019), annexed hereto as Exhibit 10.

⁴² *Id.*

⁴³ *Id.*

⁴⁴ SiteImprove’s Privacy Policy, obtained via <https://siteimprove.com/en/privacy/privacy-policy/> (last accessed April 30, 2019), annexed hereto as Exhibit 11.

**DEFENDANTS ARE ENRICHED FROM MAKING THESE UNLAWFUL,
UNATHORIZED, AND UNNECESSARY DISCLOSURES**

151. Defendants make the disclosures described herein for marketing purposes.

152. In exchange for disclosing PII about its patients, Defendants are compensated by the third parties with enhanced online advertising services, including but not limited to retargeting.

153. Retargeting is a form of online targeted advertising that targets users with ads based on their previous Internet actions that is facilitated through the use of tracking pixels and cookies. Once the 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.

154. For example, retargeting could allow a web-developer to show advertisements on other websites to customers or potential customers based on the specific communications exchanged by the patient or their activities on a certain website. Using the Facebook Tracking Pixel, a website could target ads on Facebook itself or the Facebook advertising network to persons for whom Facebook recorded the targeted actions. The same or similar actions can be accomplished via disclosures to the other third-parties.

155. Once personally identifiable information relating to patient communications is disclosed to third parties, Defendants lose the ability to further control its dissemination and use.

156. Upon information and belief, the third parties to whom Defendants make disclosures of patient PII use that information for the third-parties' own purposes.

157. The monetization of the data being disclosed by Defendants, both by the Defendants and the third-parties to whom the data is disclosed, demonstrates the inherent value of the information collected.

158. By sending this sensitive information to third-parties, Defendants violate Plaintiffs' and Class Members' rights in that information, namely their privacy rights to not have their personally-identifiable patient and medical information (including their status as patients and the content of communications exchanged with providers) shared without their knowledge or consent.

PLAINTIFFS' EXPERIENCES

159. Plaintiff John Doe is a patient of Partners through Mass General.

160. Plaintiff Jane Doe is a patient of Partners through Mass General, BWH, and the Dana-Farber Cancer Institute.

161. Plaintiffs John Doe and Jane Doe enjoy objectively reasonable expectations of privacy for communications with Defendants that are grounded in:

- a. Plaintiffs' status as patients and Defendants' status as Plaintiffs' health care providers;
- b. Defendants' common law obligations to maintain the confidentiality of communications with patients;
- c. State and federal laws protecting the confidentiality of patient communications and medical information; and
- d. Defendants' express promises.

162. Plaintiff John Doe exchanged communications with Defendants Partners and Mass General via the Mass General website, including using the website to create an account on Defendants' Patient Portal, identifying himself to Defendants as a patient, and exchanging communications relating to his particular providers and medical conditions.

163. Plaintiff Jane Doe exchanged communications with Defendants Partners, Mass General, Brigham, and Dana-Farber via the respective websites, including using the websites to

create an account on Defendants' patient portal, identifying herself to Defendants as a patient, and exchanging communications relating to her particular providers and medical conditions.

164. Defendants disclosed Plaintiffs John Doe's and Jane Doe's communications, including patient status and personally identifiable information associated with these communications to third-parties.

165. Upon information and belief, Defendants were compensated for these disclosures by the third-party recipients in the form of enhanced marketing services.

166. Defendants did not pay or offer to pay Plaintiffs for their communications or personally-identifiable information associated with these disclosures before or after the disclosures were made.

167. Defendants profited from Plaintiffs' information without ever intending to compensate Plaintiffs or inform them that the disclosures had been made.

168. Defendants were unjustly enriched by their conduct.

169. Defendants violated Plaintiffs' rights to privacy in their personally identifiable sensitive, confidential medical communications.

170. Defendants' conduct injured Plaintiffs and will continue to injure Plaintiffs.

171. Injuries to Plaintiffs are ongoing due to Defendants' conduct because, upon information and belief, Plaintiffs' information continues to be disseminated, sold, and used by third-parties to target Plaintiff for specific advertising, goods, or services based on private information and communications with their health care providers.

172. Plaintiffs did not receive the full benefit of being patients of Defendants, primarily because Defendants breached their duty of confidentiality and violated Plaintiff's right to privacy.

173.

CLASS ACTION ALLEGATIONS

174. Defendants' conduct violates the law and breaches their express privacy promises.
175. Defendants' unlawful conduct has injured Plaintiffs and Class Members.
176. Defendants' conduct is ongoing.
177. Plaintiffs bring this action individually and as a class action against Defendants.
178. Plaintiffs seek class certification for the following proposed Class and subclasses:

The Partners Healthcare Class

During the fullest period allowed by law, all Massachusetts residents who are, or were, patients of Partners Healthcare or any of its affiliates and who exchanged communications at www.massgeneral.org, www.brighamandwomens.org, www.dana-farber.org, or any other Partners Healthcare-affiliated website that causes disclosures of patient information and communications to be made to third-parties.

The Mass General Subclass

During the fullest period allowed by law, all Massachusetts residents who are, or were, patients of Mass General and who exchanged communications at www.massgeneral.org.

The Brigham Subclass

During the fullest period allowed by law, all Massachusetts residents who are, or were, patients of Brigham and Women's Hospital and who exchanged communications at www.brighamandwomens.org.

The Dana-Farber Subclass

During the fullest period allowed by law, all Massachusetts residents who are, or were, patients of Dana-Farber and who exchanged communications at www.dana-farber.org.

179. Excluded from the proposed Class or Subclasses are: (a) any Judge presiding over this action and members of their families; (b) Defendants; (c) any entity in which any Defendant has a controlling interest or which has a controlling interest in any Defendant; (d) the officers and directors of Defendants; and (e) Defendants' legal representatives, assigns, and successors; (f) all counsel for any party to this action; and (g) all persons who properly execute and file a

timely request for exclusion from the Class.

180. Plaintiffs reserve the right to redefine the Class and/or add Subclasses at, or prior to, the class certification stage; in response to discovery; or pursuant to instruction by the Court.

181. This action is properly maintainable as a class action as specifically defined in Massachusetts Rule of Civil Procedure 23.

182. **Numerosity:** While the exact number of Class Members cannot yet be determined, the Class consists at a minimum of hundreds of people dispersed throughout the State of Massachusetts, such that joinder of all members is impracticable. The exact number of Class Members can be determined by review of information maintained by Defendants.

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

a. whether Defendants' practices relating to disclosures of Plaintiffs and Class Members' communications with Defendants to third-party companies attached to personally identifiable information was intentional;

b. whether Defendants profited from the disclosures to third-parties;

c. whether Defendants' practices relating to disclosures of Plaintiffs' and Class Members' communications with Defendants to third-party companies attached to personally identifiable information violates Massachusetts General Law, chapter 214, § 1B;

d. whether Defendants' practices relating to contemporaneous disclosures of Plaintiffs' and Class Members' communications with Defendants to third-party companies attached to personally identifiable information violates Massachusetts General Law, chapter 272, § 99;

- e. whether Defendants' practices violate Massachusetts General Law, chapter 111, § 70E;
- f. whether Defendants' practices constitute a breach of fiduciary duty;
- g. whether Defendants' conduct harmed and continues to harm Plaintiffs and Class Members, and, if so, the extent of injury;
- h. whether and to what extent Plaintiffs and Class Members are entitled to damages and other monetary relief;
- i. whether and to what extent Plaintiffs and Class Members are entitled to equitable relief including, but not limited to, a preliminary and/or permanent injunction; and;
- j. whether and to what extent Plaintiffs and Class Members are entitled to attorneys' fees and costs.

184. **Adequacy of Representation:** Plaintiffs are committed to prosecuting this action and have retained competent counsel experienced in litigation of this nature. Plaintiffs' claims are coincident with, and not antagonistic to, those of the other Class Members they seek to represent. Plaintiffs have no disabling conflicts with Class Members. Accordingly, Plaintiffs are adequate representative of the Classes and, along with counsel, will fairly and adequately protect the interests of the Class and Subclasses.

185. **Typicality:** Plaintiffs' claims are typical of the claims of other Class Members and Plaintiffs have substantially the same interest in this matter as other Class Members. Plaintiffs have no interests that are antagonistic to, or in conflict with, the interests of the other members of the Class. Plaintiffs' claims arise out of the same set of facts and conduct as all other Class Members. Plaintiffs and all Class Members are patients of the Defendants who used the websites set-up by the Defendants for patients, and are victims of the Defendants' respective

unauthorized disclosures to third-parties. All claims of the Plaintiffs and Class Members are based on Defendants' wrongful conduct and unauthorized disclosures.

186. Defendants will continue to commit the violations alleged, and Plaintiffs and Class Members will be subject to and continue to suffer from the same or substantially similar conduct.

187. Defendants have acted or refused to act on grounds generally applicable to the entire Class, thereby making final injunctive relief or corresponding declaratory relief appropriate.

188. The common questions of law and fact predominate over any questions affecting only the individual Class Members and a class action is the superior method for fair and efficient adjudication of the controversy. Although many Class Members have claims against Defendants, the likelihood that individual Class Members will prosecute separate actions is remote due to the time and expense necessary to conduct such litigation. Serial adjudication in numerous venues is not efficient, timely, or proper. Judicial resources would be unnecessarily depleted by prosecution of individual claims. 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 Defendants 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 Members who are not parties to the adjudications. If a class action is not permitted, Class Members will continue to suffer losses and Defendants' misconduct will continue without proper remedy.

189. Plaintiff anticipates no unusual difficulties in the management of this litigation as a class action. The Class and Subclasses are readily ascertainable and direct notice can be provided from the records maintained by Defendants, electronically or by publication, the cost of

which is properly imposed on Defendants.

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

CLAIMS FOR RELIEF

COUNT I – INTERCEPTION OF WIRE COMMUNICATIONS IN VIOLATION OF MASSACHUSETTS GENERAL LAW c. 272, § 99 **(Plaintiffs Individually and On Behalf of the Class and Subclasses)**

191. Plaintiffs incorporate all other paragraphs as if fully stated herein.

192. Massachusetts General Law c. 272, § 99 prohibits any person from willfully and secretly intercepting the contents of any wire communication through the use of any intercepting device unless given prior authority by all parties to a communication to do so.

193. Any person aggrieved by a violation of G.L. c. 272, § 99 “shall have a civil cause of action against any person who so intercepts, discloses, or uses such communications or who so violates his personal, property, or privacy interest.”

194. All Defendants qualify as persons under the statute.

195. All communications between Plaintiffs or Class Members and Defendants qualify as wire communications under Massachusetts law because each communication is made using personal computing devices (*e.g.*, computers, smartphones, tablets) 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.

196. An “interception” under the statute “means to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire ... communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication[.]” § 99B(4).

197. Defendants engaged and continue to engage in an “interception” by aiding others

(including Facebook and Google) to secretly record the contents of Plaintiffs' and Class Members' wire communications.

198. An "intercepting device" is "any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire ... communication[.]" § 99B(3) (setting forth exceptions that do not apply here).

199. The "intercepting devices" used in this case include, but are not limited to:

- a. Plaintiffs' and Class Members' personal computing devices;
- b. Plaintiffs' and Class Members' web-browsers;
- c. Plaintiffs' and Class Members' browser-managed files;
- d. Internet cookies;
- e. Defendants' own computer servers;
- f. the third-party source code utilized by Defendants; and
- g. the computer servers of the third-parties to which Plaintiffs and Class

Members' communications were re-directed.

200. Under the statute, "contents" is defined to mean "any information concerning the identity of the parties to such communication or the existence, contents, substance, purport, or meaning of that communication." § 99B(5).

201. Defendants aided in and continue to aid in the interception of contents in that the data from the communications exchanged between Plaintiffs or Class Members and Defendants that were re-directed to and recorded by the third-parties include information which identifies the parties to each communication, their existence, and their exact contents.

202. Under the statute, aggrieved persons are "entitled to recover ... (1) actual damages but not less than liquidated damages computed at the rate of \$100 per 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 disbursements reasonably incurred.”

203. In addition to statutory damages, Plaintiffs and Class Members were damaged by Defendants’ breach in that:

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

b. Defendants 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;

c. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendants’ duty to maintain confidentiality.

COUNT II – INVASION OF PRIVACY IN VIOLATION OF
MASSACHUSETTS GENERAL LAW c. 214, § 1B
(Plaintiffs Individually and On Behalf of the Class and Subclasses)

204. Plaintiffs incorporate all other paragraphs as if fully stated herein.

205. Massachusetts General Law c. 214, § 1B provides that “a person shall have a right against unreasonable, substantial, or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such a right and in connection therewith to award damages.”

206. All health care providers owe their patients a duty not to disclose medical information about the patient without the patient’s informed consent.

207. Massachusetts G.L. c. 111, §70E provides that every patient or resident of a Massachusetts health care facility shall have the right “to confidentiality of all records and communications to the extent provided by law.”

208. The confidentiality of the patient-provider relationship is a cardinal rule of the

medical professional which has come to be justifiably relied upon by patients seeking advice and treatments.

209. Plaintiffs and Class Members are patients of Defendants.

210. Defendants owe Plaintiffs and Class Members a duty of confidentiality.

211. Despite their duty not to disclose without informed consent, Defendants disclosed information relating to Plaintiffs' and Class Members' medical treatment to third-parties without their knowledge or informed consent.

212. The information disclosed included personally identifiable information, Plaintiffs' and Class Members' status as patients of Defendants, and the exact contents of communications exchanged between Plaintiffs or Class Members with Defendants, including but not limited to information about log-ins to Defendants' patient portal, treating doctors, potential doctors, conditions, treatments, appointments, search terms, and bill payment.

213. The disclosure of personally identifiable medical information constitutes an unreasonable, substantial, and serious interference with Plaintiffs' and Class Members' rights to privacy.

214. Plaintiffs and Class Members were damaged by Defendants' breach in that:

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

b. Defendants 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;

c. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendants' duty to maintain confidentiality.

COUNT III – BREACH OF FIDUCIARY DUTY
(Plaintiffs Individually and On Behalf of the Class and Subclasses)

215. As medical providers for Plaintiffs and Class Members, Defendants owe Plaintiffs and Class Members a fiduciary duty of confidentiality in the data and content of communications exchanged between Defendants and the Plaintiffs or Class Members.

216. Defendants breached their duty of confidentiality by disclosing personally identifiable information about Plaintiffs' and Class Members' status as patients and the exact content of their communications, including but not limited to information about log-ins to Defendants' patient portals, treating doctors, potential doctors, conditions, treatments, appointments, search terms, and bill payment.

217. Plaintiffs and Class Members were damaged by Defendants' breach in that:

- a. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private;
- b. Defendants 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;
- c. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendants' duty to maintain confidentiality.

218. All conditions precedent to this action have been performed or have occurred.

PRAYER FOR RELIEF

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

- a. General damages for the violation of Plaintiffs' and Class Members'

privacy in an amount to be determined by a jury without reference to specific harm;

b. Benefit of the bargain damages representing the difference between the amount Plaintiffs' and Class Members paid for medical care that was required to remain private versus the value of medical care that disclosed personal, private, confidential information and, thus, was not entirely private;

c. Statutory damages of \$1,000 per Plaintiff and Class Members pursuant to Mass. G.L. c. 272, § 99;

d. A reasonable royalty for Defendants' misappropriation of Plaintiffs' and Class Members' information without consent;

e. Imposition of a constructive trust against Defendants through which Plaintiffs and Class Members can be compensated for any unjust enrichment gained by Defendants;

f. Nominal damages for violation of Plaintiffs' and Class Members' legal rights to privacy;

g. Attorney's fees and litigation costs reasonably expended; and

h. 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 Defendants from making any further disclosures of the Plaintiffs' or Class Members' communications to third-parties without the Plaintiffs' or Class Members' express, informed written consent.

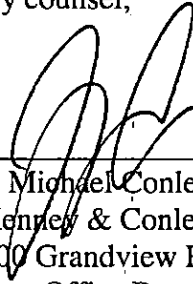
DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Respectfully submitted,

JOHN DOE, II,

By counsel,



J. Michael Conley BBO# 094090
Kenney & Conley, P.C.
100 Grandview Road, Suite 218
Post Office Box 9139
Braintree, MA 02185-9139
781-848-9891
michael@kenneyconley.com

DATED: May 23, 2019