Ronald A. Marron (175650)
Alexis M. Wood (270200)
Kas L. Gallucci (288709)
LAW OFFICES OF RONALD A. MARRON
651 Arroyo Drive
San Diego, CA 92103
Telephone: (619) 696-9006
Facsimile: (619) 564-6665
ron@consumersadvocates.com
alexis@consumersadvocates.com
kas@consumersadvocates.com

Christian Levis (*pro hac forthcoming*)
Amanda Fiorilla (*pro hac forthcoming*)
Rachel Isabel Kesten (*pro hac vice forthcoming*)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com
rkesten@lowey.com

[*additional counsel on signature page*]

SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF LOS ANGELES

LAUREN DANCHICK, individually and on behalf of all others similarly situated,

Plaintiff,

v.

PLANNED PARENTHOOD LOS ANGELES, a California nonprofit public benefit corporation, and PLANNED PARENTHOOD FEDERATION OF AMERICA, INC., a New York not-for-profit corporation,

Defendants.

Case No: 21STCV46871

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Lauren Danchick, individually and on behalf of all others similarly situated, asserts the following against Defendants Planned Parenthood Los Angeles and Planned Parenthood Federation of America, Inc. (collectively, "Planned Parenthood" or "Defendants") based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

INTRODUCTION

1. Planned Parenthood Federation of America, Inc. ("PPFA") proclaims to be the nation's leading provider of affordable health care for women, men, and young people. PPFA provides a wide range of sexual and reproductive health care to millions of people through a national network of more than 600 health centers and clinics operated by their regional affiliates.

2. Planned Parenthood Los Angeles ("PPLA") is a member-affiliate of PPFA, and is one of the largest providers of comprehensive, reproductive health care services in Los Angeles County.

3. In connection with its reproductive health care services, PPLA promises to protect its patients' health information and comply with any legal or regulatory requirements.

4. For instance, PPLA promises that it "understand[s] that health information about you and your health care is personal" such that it is "committed to protecting health information about you."[1] PPLA has a "pledge" in which it promises to maintain the confidentiality of patients' medical information that is "backed-up by federal and state law."

5. PPFA makes similar representations to patients, stating that it "respect[s] and [is] committed to protecting the privacy of users."[2]

6. Given the extremely confidential and sensitive nature of the medical services that Planned Parenthood provides to patients—and Planned Parenthood's representations—Plaintiff and Class members reasonably expected that Planned Parenthood's data security practices

[1] *See* Privacy Policy, Planned Parenthood Los Angeles, https://www.plannedparenthood.org/planned-parenthood-los-angeles/hipaa (last visited Dec. 8, 2021).

[2] *See* Privacy Policy, Planned Parenthood, https://www.plannedparenthood.org/privacy-policy (last visited Dec. 8, 2021).

complied with relevant laws, regulations, and industry standards, and would be sufficient to protect the type of sensitive information they collected and stored.

7. But these representations were false. Planned Parenthood did not maintain adequate data security designed to protect the highly sensitive and confidential nature of Plaintiff' and Class members' personal and medical information.

8. On October 17, 2021, PPLA identified suspicious activity on its computer network. Despite knowing that its systems had been compromised since mid-October, PPLA waited until November 30, 2021 to notify patients of the data breach (the "Data Breach Notice Letter"). Attached hereto s **Exhibit A** is a copy of the Data Breach Notice Letter transmitted to its patients.

9. The Data Breach Notice Letter explained that an "unauthorized person" gained access to their network between October 9 – 17, 2021 (the "Breach Period"). The unauthorized person "exfiltrated" files from their systems, including patient names, dates of birth, addresses, and protected health information, including insurance identification numbers, and clinical information, such as diagnosis, treatment, or prescription information (collectively the "e-PHI"). The data breach is estimated to have impacted approximately 400,000 patients.

10. The Data Breach Notice Letter downplayed the severity of the intrusion and conveniently failed to notify patients that the data breach was caused by ***malware/ransomware***, which is a computer code ***intentionally designed*** to infiltrate systems and gain access to private and sensitive information.

11. Instead, the Data Breach Notice Letter stated that there was "no evidence that any information . . . has been used for fraudulent purposes" and that patients were only being notified out of "an abundance of caution." But these assurances have no basis in fact, as PPLA cannot know what these hackers have done (or intend to do) with Plaintiff's and Class members' e-PHI once it was exfiltrated from its systems. Indeed, PPLA contradicts its own statement by then encouraging patients to "review statements you receive from your health insurer and health care providers" given the risk of medical fraud that Plaintiff and Class members now face.

12. Doubling down on these omissions and misstatements, John M. Erickson, a spokesman for PPLA, boldly stated there is "no indication this was a targeted attack," despite that

the attack used malicious code designed explicitly for this purpose.

13. Despite PPLA's desire to downplay the severity of the data breach, it has caused immediate, substantial harm to Plaintiff and Class members.

14. Medical information, like the highly sensitive and confidential e-PHI compromised here, is some of the most sensitive forms of personal information, as it is immutable and cannot be changed. Planned Parenthood's egregious handling of this confidential and sensitive e-PHI, which is now in the hands of bad actors, constitutes an extreme invasion of privacy. Patients consistently recognize the importance of protecting medical information. A survey by the *Institute for Health Freedom* found that 78% of patients feel it is "very important" that their medical records be kept confidential. As a result of the data breach, Plaintiff and Class members no longer have control over their e-PHI, which is now forever in the hands of bad actors.

15. Plaintiff and Class members also have experienced emotional distress as a result of the data breach because their e-PHI is now in the hands of bad actors with illicit motives, such as publicly disclosing this information. Bad actors may attempt to "dox" Plaintiff and Class members, publishing their names, home addresses, and reasons why they went to Planned Parenthood online. The threat of this action in and of itself is emotionally distressing, as many of their friends, loved ones, and family members may not be aware of their specific treatment at Planned Parenthood. As a result of the data breach, they are constantly in a state of fear and/or distress that this information may be made publicly available or extorted against them.

16. Plaintiff and Class members are now at an immediate risk of online and even physical harassment, threats, intimidation, and retribution for visiting a Planned Parenthood clinic, especially as their home addresses were disclosed in connection with their sensitive medical information.

17. Anti-Planned Parenthood actors are known to target facilities, doctors, and patients. In October 2020, a demonstration outside the Planned Parenthood clinic in Walnut Creek, California took a violent turn when armed security guards hired by anti-abortion activists pepper-sprayed counter protesters. The *National Abortion Federation* ("NAF") in their 2019 Violence and Disruption Statistics (the most recent year statistics are available) found that internet harassment

rose and hate mail and harassing phone calls more than doubled with providers reporting 3,123 targeted incidents of hate mail and harassing phone calls, rising from 1,388 in 2018. According to the NAF, abortion care providers and staff continued to receive focused threats through phone calls and text messages as well as postal mail and flyers sent not only to health care facilities, but also to their homes. This hate speech often escalates and turns into death threats and threats of harm.

18. As a result of the data breach, Plaintiff and Class members have suffered emotional distress, trauma, elevated stress, and anxiety, and remain in constant fear of retaliation, harassment, and other acts of retribution.

19. Further, given the highly sensitive and confidential nature of the e-PHI compromised by hackers in a malicious attack (i.e., through malware/ransomware), Plaintiff and Class members will be required to expend significant time and effort to mitigate the effects of the data breach, such as monitoring their credit reports and accounts for fraud.

20. This risk is ongoing because, unlike a credit card, there is no way to cancel e-PHI. The U.S. Department of Health and Human Services ("HHS") has identified several imminent risks as a result of hackers obtaining patients' e-PHI including: (1) medical identity theft, i.e., the use of a patients' medical information to obtain medical services, such as medical prescriptions, surgery, or other medical treatment, as well as counterfeit settlements against health insurers; (2) the weaponization of medical data, i.e., the use of medical data to threaten, extort, or influence the patient to extort money or disparage someone; (3) financial fraud, i.e., the use of e-PHI to create credit card or bank accounts in the patients' name, taking out loans or lines of credit in the patients' name, or the filing of fraudulent tax documents or insurance information; and (4) cyber campaigns, using the medical data in combination with other information on the dark web to commit fraud, identity theft, conduct phishing or scams, or obtain the patients' credentials for other services. The "unauthorized person" who breached Planned Parenthood's systems can continue to exploit this information at the expense of Plaintiff and the Class. This ongoing imminent risk can often persist for years, as identity thieves often hold stolen data for long periods of time before using it.

21. Such careless handling of e-PHI is prohibited by federal and state law. For example,

the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires healthcare providers, like Planned Parenthood, and their business associates to safeguard patient e-PHI through a multifaceted approach that includes, among other things: (a) ensuring the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit; (b) proactively identifying and protecting against reasonably anticipated threats to the security or integrity of e-PHI; (c) protecting against reasonably anticipated, impermissible uses or disclosures of e-PHI; (d) putting in place the required administrative, physical and technical safeguards to protect e-PHI; (e) implementing policies and procedures to prevent, detect, contain, and correct security violations; (f) effectively training their workforce regarding the proper handling of e-PHI; and (g) designating individual security and privacy officers to ensure compliance with these policies and procedures.

22. Planned Parenthood's failure to comply with HIPAA and other laws and/or guidelines as alleged herein by, among other things, failing to take reasonable steps to safeguard patients' highly sensitive and confidential e-PHI, has directly resulted in injury to Plaintiff and the Class.

23. Given the secret nature of, among other things: (a) Planned Parenthood's policies, procedures, systems, and controls; (b) the result of the "investigation" into the data breach disclosed in the Data Breach Notice Letter; and (c) communications among Planned Parenthood and/or the "third-party cybersecurity firm [who] was engaged to assist in [their] investigation" concerning the data breach referenced in the Data Breach Notice Letter, Plaintiff believes that further evidentiary support for their claims will be unearthed after a reasonable opportunity for discovery.

24. Plaintiff and Class members bring claims for invasion of their privacy interests, as established through California's privacy laws and California's Constitution. In addition, Planned Parenthood's actions constitute negligence, breach of contract and implied contract, unjust enrichment, as well as violations of several state consumer protection and privacy laws.

25. Plaintiff seeks to remedy these harms on behalf of themselves and all similarly situated individuals whose highly sensitive and confidential e-PHI was stolen in the data breach.

Plaintiff and Class members seek remedies including but not limited to statutory damages, compensatory damages, and injunctive relief requiring substantial improvements to Planned Parenthood's security systems.

PARTIES

I. PLAINTIFF

26. Plaintiff **Lauren Danchick** ("Plaintiff Danchick") is a natural person and citizen of California and a resident of Los Angeles County. Plaintiff Danchick received medical treatment at the Planned Parenthood Los Angeles Canoga Park clinic for women's healthcare services in 2020.

27. Plaintiff Danchick provided Planned Parenthood with her highly sensitive and confidential e-PHI, including her name, date of birth, address, insurance information, and medical history. Records reflecting Plaintiff Danchick treatment contained additional personal and highly sensitive e-PHI, including the reason(s) for her visit and treatment information. This information, along with other e-PHI associated with Plaintiff Danchick''s treatment was stored electronically on Planned Parenthood's servers during the Breach Period and as described below, was accessed and exfiltrated without her consent.

28. On or about November 30, 2021**,** Planned Parenthood Los Angeles notified Plaintiff Danchick that her highly sensitive and confidential e-PHI was compromised as a result of the data breach.

29. Given that Plaintiff Danchick's highly sensitive and confidential e-PHI was accessed and exfiltrated without her consent as a result of the data breach, Plaintiff Danchick has suffered concrete harm, including: (1) the unauthorized disclosure of her private health information to third parties; (2) the imminent risk of fraud and identity theft; (3) the intrusion upon seclusion and violation of her reasonable expectation of privacy in such highly sensitive medical information, such as that related to her medical history and treatment; (4) and the increased risk of the threat of online and physical harassment and retribution for utilizing Planned Parenthood's reproductive health care services; and (5) emotional distress.

II. DEFENDANTS

A. PPFA

30. Defendant **Planned Parenthood Federation of America, Inc**. ("PPFA") is a New York not-for-profit corporation with principal executive offices located at 123 William Street, New York, NY 10038.

31. PPFA is the leading national organization dedicated to offering affordable health care services, public education, and advocacy in the field of reproductive health care. PPFA's core mission is to ensure the provision of high-quality, non-judgmental comprehensive reproductive health care services, to provide educational programs relating to reproductive and sexual health, and to advocate for public policies to ensure access to health services—including for individuals with low incomes or from underserved communities. PPFA also engages in public education about, and advocacy in favor of, the right to access safe and legal abortions.

32. PPFA is a membership organization composed of more than fifty affiliate organizations, with a Board of Directors. The member-affiliates are responsible for setting the long-range goals and priorities of PPFA and for electing the PPFA Board of Directors. Through their participation and voting, PPFA's member-affiliates control the mission and direction of PPFA. Historically PPFA's member affiliates were required to contribute financially to PPFA. Each affiliate of PPFA has the right to use the Planned Parenthood name and service mark.

33. Cumulatively, PPFA's member-affiliates operate more than 600 health centers that provide a wide range of reproductive health care services and education. Among them are contraception (including long-acting reversible contraceptives ("LARCs")), contraceptive counseling, physical exams, clinical breast exams, screening for cervical and testicular cancers, testing and treatment for sexually transmitted infections ("STIs"), treatment of sexual dysfunction in men, pregnancy testing and counseling, pre-natal care, testing and treatment for HIV, gender affirming care including hormone therapy for transgender patients, some sterilization services (including vasectomies), colposcopies, abortion, and health education services. PPFA's affiliates also provide referrals for these services if they are unable to provide them at their health centers.

34. In 2019, Planned Parenthood affiliates provided more than 10.4 million services to

approximately 2.4 million patients. Planned Parenthood affiliates provided more than 5.4 million STI testing and treatment services, more than 2.5 million contraceptive services, administered more than 598,000 cancer screenings and preventive services such as breast exams and cervical screens (Pap tests), conducted more than 860,000 HIV tests, and performed more than 350,000 abortions.

35. An estimated one out of every three women nationally has received care from a Planned Parenthood affiliate at least once in her life.

B. PPLA

36. Defendant **Planned Parenthood Los Angeles** ("PPLA") is a California nonprofit public benefit corporation with principal executive offices located at 400 W. 30th Street, Los Angeles, CA 90007.

37. PPLA is a member-affiliate of PPFA. PPLA utilizes the Planned Parenthood name and service mark on its website, messaging, and communications, including on the Data Breach Notice Letter sent to Plaintiff and the Class. In addition, the CEO of PPLA, Susan Dunlap, is a member of PPFA's Board of Directors.

38. According to PPLA, its mission "is to provide convenient and affordable access to a comprehensive range of quality reproductive health care and sexual health information through patient services, education and advocacy."

39. PPLA is one of the largest providers of comprehensive, reproductive health care services in Los Angeles County. PPLA's reproductive health care services include but are not limited to, pregnancy testing and services, STI testing and treatment, contraception services, abortion and emergency contraception, as well as general men's, women's, and LGBT health care services.

40. PPLA operates twenty-one California (21) health centers. Of the women, men, and young people who rely on PPLA for care, 84% receive family planning services and 78% are living at or below the federal poverty level.

41. PPLA represents that "Planned Parenthood providers are among the best-trained and most experienced in the field of reproductive health care" and that it "offer[s] a level of

nonjudgmental care that's hard to find anywhere else." Further, PPLA pledges to protect its patients' health information and comply with any legal or regulatory requirements. PPLA states that it "understand[s] that health information about you and your health care is personal" such that it is "committed to protecting health information about you." PPLA's pledge promises to maintain the confidentiality of patients' medical information that is "backed-up by federal and state law." However, despite this pledge, PPLA failed to secure its patients highly sensitive and confidential e-PHI, which has been exfiltrated which was seen by unauthorized third parties and can now be weaponized and used to harass and threaten the patients who used its services.

42. Upon information and belief, PPLA and PPFA share common servers, networks, systems, databases, and/or healthcare and patient management systems.

43. PPLA and PPFA are collectively referred to throughout the Complaint as "Planned Parenthood" or "Defendants."

JURISDICTION AND VENUE

44. Jurisdiction is proper in the Superior Court of Los Angeles pursuant to California Code of Civil Procedure § 410.10.

45. This Court has personal jurisdiction over PPLA because PPLA maintains its principal executive offices in Los Angeles, California and is a registered California corporation.

46. This Court has personal jurisdiction over PPFA because PPFA has sufficient minimum contacts in California. For example, PPFA purposefully availed itself of the privileges and benefits associated with conducting business in this state, by, among other things, reaching into California to establish an affiliated partnership with its PPFA member-affiliate—PPLA. Under PPFA's bylaws, historically PPFA's member-affiliates, including PPLA are also required to contribute financially to PPFA, and affiliate dues contribute to PPFA's financial support. PPFA allows its affiliates, including PPLA the right to use the Planned Parenthood name and service mark in California, which PPLA displays on its website. Further, upon information and belief, PPFA shares common servers, networks, systems, databases, and/or healthcare and patient management systems with PPLA.

47. Venue is proper in this Court because Defendants transact business in this County,

PPLA's principle executive offices are located in this County, and a substantial portion of the events giving rise to the claims occurred within this County, including the data breach on PPLA's network that permitted unauthorized third-parties to obtain the confidential and sensitive e-phi of approximately 400,000 of PPLA's patients.

FACTUAL BACKGROUND

III. THE PLANNED PARENTHOOD DATA BREACH

48. In connection with its services, PPLA has consistently promised patients that it pledges to protect its patients' health information and comply with any legal or regulatory requirements. For instance, PPLA promises that it "understand[s] that health information about you and your health care is personal" such that it is "committed to protecting health information about you."[3] As part of PPLA's "pledge," it promises to maintain the confidentiality of patients' medical information and that it is "backed-up by federal and state law."

49. PPLA has dedicated a section on its website to apprise its patients, including Plaintiff and Class members, of the permissible uses and disclosure of their medical records.

50. More specifically, PPLA posts on its website a "HIPAA Privacy Policy | NOTICE OF HEALTH INFORMATION PRIVACY PRACTICES" dated September 1, 2014 (the "Privacy Policy"), which PPLA admits they are required to comply with. In its Privacy Policy, PPLA pledges to protect its patients' health information and states "[w]e understand that health information about you and your health care is personal. We are committed to protecting health information about you."

51. Specifically, PPLA's "pledge" states "[o]ur pledge regarding your health information is backed-up by federal and state law. The privacy and security provisions of the federal Health Insurance Portability and Accountability Act ("HIPAA") require us to: Make sure that health information that identifies you is kept private; Make available this notice of our legal duties and privacy practices with respect to health information about you; and Follow the terms of

[3] *See* Privacy Policy Planned Parenthood Los Angeles, https://www.plannedparenthood.org/planned-parenthood-los-angeles/hipaa (last visited Dec. 8, 2021).

the notice that is currently in effect."

52. These promises were false. As a result of Planned Parenthood's deficient data security, between October 9 – 17, 2021, unauthorized third parties using malicious code, i.e., malware and ransomware, gained access and exfiltrated Plaintiff's and Class members' highly sensitive and confidential e-PHI. As a result, these unauthorized third parties have seen Plaintiff's and Class members highly sensitive and confidential e-PHI.

53. Week a month later, on November 30, 2021, PPLA finally notified patients, including Plaintiff, of the data breach and that their highly sensitive and confidential e-PHI was compromised.

54. PPLA determined that the "unauthorized person" installed malware/ransomware to gain access to its network and exfiltrated files from its systems. Ransomware is a malicious computer code intentionally designed to block an organization's access to its own computer network to extort a ransom. Malware is malicious computer code explicitly designed to exfiltrate files or otherwise cause harm to computer networks.

55. PPLA determined that the files exfiltrated by bad actors included patients' names, and one or more of the following: dates of birth, addresses, and protected health information including insurance identification numbers, and clinical data, such as diagnosis, treatment, or prescription information.

56. While PPLA's "Notice of Patient Privacy Incident" included on its website indicates that the unauthorized person "installed malware/ransomware and exfiltrated some files from our systems," PPLA's Data Breach Notice Letter to Plaintiff downplays the intrusion and fails to include the relevant information that malware/ransomware was installed. This is especially problematic as malware and ransomware are notoriously used by bad actors with malintent.

57. The cyber criminals who committed the data breach viewed, obtained, and exfiltrated Plaintiff's and Class members' highly sensitive and confidential e-PHI for malicious purposes and now have it available to them to sell to other bad actors or otherwise misuse the information, including "doxing" Plaintiff and Class members. This "doxing" can include publishing their names, home addresses, and reasons why they went to Planned Parenthood online.

58. Significantly, Planned Parenthood does not represent that Plaintiff's and Class members' e-PHI was encrypted, password protected, or secured in some other manner that would prevent the malicious actors from actually using the information. Upon information and belief, these malicious actors who gained Plaintiff's and Class members' e-PHI now have unfettered access.

IV. PLANNED PARENTHOOD'S HISTORY OF DATA BREACHES

59. This is not the first time PPFA, or its affiliates experienced a data breach as a result of their severely deficient data security. PPFA and its affiliates have been the target of hackers and anti-abortion groups for many years because of its status as a prominent nationally recognized organization that advocates for reproductive rights.

60. In July 2015, PPFA was targeted by a group of hackers called "3301" who gained access to the names and contact information, including email addresses and passwords, of hundreds of PPFA employees across the nation. The 3301 hackers also planned to deface the PPFA website and "dump" multiple of their databases, i.e., expose it to the public. The 3301 hackers then exposed the users' usernames, emails, and passwords.

61. In 2020, PPFA's software vendor, Blackbaud, Inc., experienced a data breach between February 7 and May 20, 2020 that compromised the personal information of donors of several affiliated Planned Parenthoods. The perpetrators of that attack held the data for ransom.

62. Most recently, on April 9, 2021, PPFA member-affiliate Planned Parenthood of Metropolitan Washington D.C., revealed that it suffered a data breach between August 27, 2020 and October 8, 2020, whereby unauthorized actors gained access to their network and acquired patient and donor data for an undisclosed number of people. The data compromised included names, addresses, dates of birth, diagnoses, treatments, prescription information, social security numbers, and financial information. Additionally, among the leaked documents were check images with donor's names, bank account, and routing numbers. In addition to patient information, the leaked donor information provided those bad actors additional ammunition to weaponize the leaked data as it exposed those who had contributed to reproductive rights causes as targets for harassment and intimidation.

63. Given the numerous instances in which Planned Parenthood has failed to protect patients and employees, it was on notice that its data security systems were deficient. Despite this, Planned Parenthood has continued to maintain woefully deficient data security, which resulted in Plaintiff's and Class members' highly sensitive and confidential e-PHI being compromised by bad actors.

V. PLANNED PARENTHOOD FAILED TO COMPLY WITH HIPAA, THE NATIONAL STANDARD FOR PROTECTING PRIVATE HEALTH INFORMATION

64. HIPAA requires the healthcare industry to have a generally accepted set of security standards for protecting health information. HIPAA defines Protected Health Information ("PHI") as individually identifiable health information and e-PHI that is transmitted by electronic media or maintained in electronic media. This protected information includes: names, dates, phone numbers, fax numbers, email addresses, SSNs, medical record numbers, health insurance beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers, device identifiers and serial numbers, URLs, IP addresses, biometric identifiers, photographs, and any other unique identifying number, characteristic, or code.

65. To this end, HHS promulgated the HIPAA Privacy Rule in 2000 and the HIPAA Security Rule in 2003. The security standards for the protection of e-PHI, known as "the Security Rule," establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' e-PHI.

66. Defendants are either an entity covered by HIPAA, *see* 45 C.F.R. § 160.102, or "business associates" covered by HIPAA, *see* 45 C.F.R. § 160.103, and therefore must comply with the HIPAA Privacy Rule and Security Rule, *see* 45 C.F.R. Part 160 and Part 164, Subparts A, C, and E.

67. HIPAA limits the permissible uses of e-PHI and prohibits the unauthorized disclosure of e-PHI. *See* 45 C.F.R. § 164.502. HIPAA also requires that covered entities implement

appropriate safeguards to protect this information. *See* 45 C.F.R. § 164.530(c)(1).

68. The electronically stored healthcare information accessed by unauthorized third parties on Planned Parenthood's servers are e-PHI under the HIPAA Privacy Rule and the Security Rule, which protects all e-PHI a covered entity "creates, receives, maintains or transmits" in electronic form. 45 C.F.R. § 160.103.

69. The Security Rule requires covered entities, including Planned Parenthood, to implement and maintain appropriate administrative, technical, and physical safeguards for protecting e-PHI. *See* 45 C.F.R. § 164.530(c)(1). Among other things, the Security Rule requires Planned Parenthood to identify and "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity of [the] information" and "[p]rotect against any reasonably anticipated uses or disclosures." 45 C.F.R. § 164.306.

70. HIPAA also obligates Planned Parenthood to implement policies and procedures to prevent, detect, contain, and correct security violations. *See* 45 C.F.R. § 164.308(a)(1)(i).

71. HIPAA further obligates Planned Parenthood to ensure that their workforce comply with HIPAA security standard rules, *see* 45 C.F.R. § 164.306(a)(4), to effectively train their workforces on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information. *See* 45 C.F.R. § 164.530(b)(1).

72. Planned Parenthood failed to comply with these HIPAA rules. Specifically, Planned Parenthood failed to put in place the necessary technical and non-technical safeguards required to protect Plaintiff's and Class members' highly sensitive and confidential e-PHI.

VI. PLANNED PARENTHOOD VIOLATED THE FTC ACT

73. Planned Parenthood was (and still is) prohibited from engaging in "unfair or deceptive acts or practices in or affecting commerce" by the Federal Trade Commission Act, 15 U.S.C. § 45. Their failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice that violates this rule.

74. In 2007, the FTC published guidelines establishing reasonable data security

practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

75. The FTC has also published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

76. Planned Parenthood was aware of and failed to follow the FTC guidelines and failed to adequately secure patients' data stored on their servers. Furthermore, by failing to have reasonable data security measures in place, Planned Parenthood engaged in an unfair act or practice within the meaning of § 5 of the FTC Act.

77. In addition to the FTC Act, Planned Parenthood had a duty to adopt reasonable data security measures in accordance with federal law under HIPAA as well as the laws of the various states in which it operates, including the CMIA

VII. PLANNED PARENTHOOD VIOLATED THEIR COMMON LAW DUTY OF REASONABLE CARE

78. In addition to obligations imposed by federal and state law, Planned Parenthood owed and continues to owe a common law duty to Plaintiff and Class members—who entrusted Planned Parenthood with their highly sensitive and confidential e-PHI—to exercise reasonable care in receiving, maintaining, storing, and deleting the e-PHI in Planned Parenthood's possession.

79. Planned Parenthood owed and continues to owe a duty to prevent Plaintiff's and Class members' highly sensitive and confidential e-PHI from being compromised, lost, stolen, accessed, or misused by unauthorized third parties. An essential part of Planned Parenthood's duty was (and is) the obligation to provide reasonable security consistent with current industry best

practices and requirements, and to ensure information technology systems and networks, in addition to the personnel responsible for those systems and networks, adequately protected and continue to protect Plaintiff's and Class members' highly sensitive and confidential e-PHI.

80. Planned Parenthood owed a duty to Plaintiff and Class members, who entrusted Planned Parenthood with their highly sensitive and confidential e-PHI, to design, maintain, and test the information technology systems that housed Plaintiff's and Class members' highly sensitive and confidential e-PHI, to ensure that the highly sensitive and confidential e-PHI in Planned Parenthood's possession was adequately secured and protected.

81. Planned Parenthood owed a duty to Plaintiff and Class members to create, implement, and maintain reasonable data security practices and procedures sufficient to protect the highly sensitive and confidential e-PHI stored in Planned Parenthood's computer systems. This duty required Planned Parenthood to adequately train employees and others with access to Plaintiff's and Class members' highly sensitive and confidential e-PHI on the procedures and practices necessary to safeguard such sensitive information.

82. Planned Parenthood owed a duty to Plaintiff and Class members to implement processes that would enable Planned Parenthood to timely detect a breach of its information technology systems, and a duty to act upon any data security warnings or red flags detected by such systems in a timely fashion.

83. Planned Parenthood owed a duty to Plaintiff and Class members to disclose when and if Planned Parenthood's information technology systems and data security practices were not sufficiently adequate to protect and safeguard Plaintiff's and Class members' highly sensitive and confidential e-PHI.

84. Planned Parenthood violated these duties. Planned Parenthood did not implement measures designed to timely detect a breach of their information technology systems, as required to adequately safeguard Plaintiff's and Class members' highly sensitive and confidential e-PHI. Planned Parenthood also violated their duty to create, implement, and maintain reasonable data security practices and procedures sufficient to protect Plaintiff's and Class members' highly sensitive and confidential e-PHI. As the Data Breach Notice Letter states, "a third-party

cybersecurity firm was engaged to assist in our investigation," ***after the breach*** occurred. Planned Parenthood should have taken these steps ***beforehand*** to protect the highly sensitive and confidential e-PHI in their possession and prevent the breach from occurring, as required under HIPAA and FTC guidelines, as well as other state and federal law and/or regulations.

85. Planned Parenthood owed a duty to Plaintiff and Class members to timely disclose the fact that a data breach, resulting in unauthorized access to their highly sensitive and confidential e-PHI, had occurred.

VIII. PLANNED PARENTHOOD FAILED TO COMPLY WITH THEIR OWN PRIVACY POLICY AND OTHER REPRESENTATIONS

86. PPLA's Privacy Policy lists the permitted uses and disclosures of patients' highly sensitive and confidential e-PHI and informs patients that e-PHI will be used for: (i) treatment; (ii) payment; (iii) healthcare operations; (iv) appointment reminders; (v) to individuals involved in their care or payment for their care; (vi) research; (vii) fundraising activities; (viii) as required by law; (ix) to avert a serious threat to health or safety; (x) military and veterans; (xi) workers' compensation; (xii) public health risks; (xiii) health oversight activities; (xiv) lawsuits and disputes; (xv) law enforcement; (xvi) inmates; and (xvii) coroners, health examiners and funeral directors.

87. PPLA's Privacy Policy further states that the "following uses and disclosures of health information will be made only with your written permission: [u]ses and disclosures of protected health information for marketing purposes; [u]ses and disclosures that constitute the sale of your protected health information; [and] [o]ther uses and disclosures of health information not covered by this Notice or the laws that apply to us."

88. Critically, none of the permissible uses in PPLA's Privacy Policy of e-PHI include granting unfettered access to unauthorized third parties who intend to misuse such information for illicit purposes.

89. PPLA's Privacy Policy further assuages patients' concerns regarding unauthorized disclosure of their personal information by allowing them to revoke any written authorizations: "[i]f you provide us permission to use or disclose health information about you, you may revoke

that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose health information about you for the reasons covered by your written authorization."

90. By these representations in the Privacy Policy, PPLA affirmatively—and misleadingly—assured patients, including Plaintiff and the Class members, that they had the ability to control the dissemination of their highly sensitive and confidential e-PHI and to restrict its use and access by third parties.

91. The Privacy Policy also expressly guaranteed PPLA would safeguard patients' highly sensitive and confidential e-PHI consistent with the applicable laws and regulations.

92. However, PPLA failed to safeguard patients' highly sensitive and confidential e-PHI in violation of their own Privacy Policy and applicable law and regulations, as confirmed by the Notice of Patient Privacy Incident, in which PPLA admits that an "unauthorized person gained access to our network between October 9, 2021 and October 17, 2021, installed malware/ransomware and exfiltrated some files from our systems during that time." In fact, PPLA failed to take any steps to safeguard Plaintiff's and Class members' highly sensitive and confidential e-PHI until after the data breach occurred.

93. PPLA failure to implement appropriate security measures and adequately safeguard Plaintiff's and Class members' highly sensitive and confidential e-PHI violated the terms of their own Privacy Policy and other representations.

IX. THE DATA BREACH DAMAGES PLAINTIFF AND CLASS MEMBERS

94. As a result of Planned Parenthood's deficient security measures, Plaintiff and Class members have been harmed by the compromise of their highly sensitive and confidential e-PHI.

95. Several criminal syndicates, including Ukraine's UNC1878 and China's Dynamite Panda, along with various state-sponsored groups, are known to target hospitals and healthcare providers based on the high value associated with e-PHI, both as a revenue stream (e.g., when sold on the dark web, or used to commit identify theft) and as a tool for executing future hacks (e.g., by impersonating users or providing information that can be useful in cracking passwords or security questions). Plaintiff reasonably anticipates that the identity of the hackers involved in the data breach will be revealed in discovery.

96. This exfiltrated highly sensitive and confidential e-PHI can be used for malicious purposes, including doxing, harassment, financial fraud, medical identity theft, identity theft, insurance fraud, and crafting convincing phishing messages. Plaintiff and Class members face an imminent risk of:

a. *medical identity theft*—the use of another person's medical information to obtain a medical service;

b. *weaponizing of medical data*—the use of sensitive medical data to threaten, harass, extort, or influence individuals;

c. *financial fraud*—the use of personally identifiable information contained in medical records to create credit card or bank or insurance profiles to facilitate financial and insurance fraud; and,

d. *cyber campaigns*—the use of medical data as complementary data in future hacking campaigns.

97. As a result, e-PHI has become increasingly valuable on the black market. In fact, it is more valuable than any other type of record on the dark web. For example, according to *Forbes*, as of April 14, 2017, the going rate for an SSN is $.010 cents and a credit card number is worth $.025 cents, but medical records containing e-PHI could be worth hundreds or even thousands of dollars. For example, in April of 2019, HHS estimated that the average price of medical records containing e-PHI ranged between $250 and $1,000.

98. The Fifth Annual Study on Medical Identity Theft conducted by the *Ponemon Institute* concluded that medical identity theft alone costs the average victim $13,500 to fix.

99. According to *The World Privacy Forum*, a nonprofit public interest group, one of the reasons for this price differential is that criminals are able to extract larger illicit profits using medical records than they are for a credit card or SSN. For example, while a credit card or SSN typically yields around $2,000 before being canceled or changed, an individual's e-PHI typically yields $20,000 or more. This is because, in addition to the fact that healthcare data and e-PHI are immutable (e.g., you cannot cancel your medical records), healthcare data breaches often take much longer to be discovered, allowing thieves to leverage e-PHI for an extended period of time.

100. Further, identity thieves can combine data stolen in the data breach with other information about Plaintiff and Class members gathered from underground sources, public sources, or even Plaintiff's and Class members' social media accounts. Thieves can use the combined data to send highly targeted phishing emails to Plaintiff and Class members to obtain more sensitive information, placing Plaintiff and Class members at further risk of harm. Thieves can use the combined data to commit potential crimes, including opening new financial accounts in Plaintiff's and Class members' names, making false insurance claims using Plaintiff's and Class members' insurance information, taking out loans in Plaintiff's and Class members' names, using Plaintiff's and Class members' information to obtain government benefits, filing fraudulent tax returns using Plaintiff's and Class members' information, obtaining driver's licenses in Plaintiff's Class members' names but with another person's photograph.

101. Researchers at HealthITSecurity.com have also reported criminals selling illicit access to compromised healthcare systems on the black market, which would give other criminals "access to their own post-exploitation activity, such as obtaining and exfiltrating sensitive information, infecting other devices in the compromised network, or using connections and information in the compromised network to exploit trusted relationships between the targeted organizations and other entities to compromise additional networks."

102. Given the value of e-PHI, health care providers such as Planned Parenthood are prime targets for cyberattacks, like the data breach that occurred here. Indeed, one recent report indicates that the number of healthcare cyberattacks in the United States has increased by 55% between 2020 and 2021 alone.

103. Furthermore, with the news of the U.S. Supreme Court taking up the politically charged Mississippi abortion law this court term and Texas's recent abortion law, abortion providers such as Planned Parenthood are likely targets for cyberattacks like the data breach that occurred here given the nature of the reproductive healthcare services they provide and the patients who utilize those services.

104. More so than in a typical healthcare data breach, cybercriminals can weaponize the highly sensitive and confidential e-PHI involved here to specifically target and harass those

patients, including Plaintiff and Class members who utilized Planned Parenthood's reproductive healthcare services.

105. In 1997, an anti-abortion extremist named Neal Horsley created a chilling website called the "Nuremberg Files." The site contained the names of about 200 working abortion providers with their approximate locations alongside GIFs of dripping blood and encouragements to "SEND US MORE NAMES!" In almost scorecard like fashion, if one of the providers was injured, his or her font color turned from black to grey. If they were killed, their name was struck through. David S. Cohen, Drexel University professor and co-author of the book Living in the Crosshairs: The Untold Stories of Anti-Abortion Terrorism, has said that publishing a list "is just another way for someone out there who wants to do harm — and we know those people exist — to get more information that facilitates their harm."

106. Plaintiff and Class members who utilized Planned Parenthood's services will now have to be on extremely high alert to protect their names and addresses (which was one of the forms of e-PHI involved in the data breach) from being made public to bad actors who may seek to threaten, harass, retaliate, or intimidate them. No patient who utilizes Planned Parenthood should have to fear for their lives or safety.

107. As to the imminent risk of fraud and identity theft, Plaintiff and Class members will be required to spend substantial amounts of time monitoring their accounts for identity theft and fraud, the opening of fraudulent accounts, disputing fraudulent transactions, and reviewing their financial affairs more closely than they otherwise would have done but for the data breach. These efforts are burdensome and time-consuming. Many Class members will also incur out-of-pocket costs for protective measures such as identity theft protection, credit monitoring fees, credit report fees, credit freeze fees, fees for replacement cards in the event of fraudulent charges, and similar costs related to the data breach.

108. The risk of identity theft and fraud will persist for years. Identity thieves often hold stolen data for months or years before using it to avoid detection. Also, the sale of stolen information on the dark web may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer. Thus, Plaintiff and Class

members must vigilantly monitor their financial accounts indefinitely.

109. PPLA acknowledges that Plaintiff and Class members face a significant risk of various types of identity theft stemming from the data breach. Attempting to shift the burden of responding to the data breach to patients, PPLA recommended to Plaintiff and affected patients that "[i]t is always a good idea to review statements you receive from your health insurer and health care providers. If you see charges for services you did not receive, please call the insurer or provider immediately." Thus, PPLA acknowledges that Plaintiff and Class members face an actual imminent risk of fraud and identity theft that requires not only immediate action but continuous, ongoing monitoring.

110. Neither PPLA or PPFA has offered any credit or identity theft monitoring to affected patients. Thus, what Planned Parenthood is doing is wholly insufficient to combat the indefinite and undeniable risk of identity theft and fraud, amongst other risks, that may continue long after the data breach.

111. Plaintiff and Class members were also harmed because they were promised services that Planned Parenthood represented would include reasonable security measures to protect their highly sensitive and confidential e-PHI but that, in reality, did not. Plaintiff and Class members would not have used Planned Parenthood's services or provided their highly sensitive and confidential e-PHI had they known that these representations were false.

112. Indeed, certain Plaintiff specifically chose to seek sensitive medical procedures at a Planned Parenthood facility because they did not feel comfortable obtaining them from their primary doctor due to concerns for their privacy and trusted that Planned Parenthood would maintain the privacy and confidentiality of their highly sensitive and confidential e-PHI.

113. Lastly, Plaintiff and Class members have been harmed by Planned Parenthood's intrusion upon their seclusion and invasion of their privacy rights, as described in Section X. Planned Parenthood configured their systems in such a way to make Plaintiff's and Class members' highly sensitive and confidential e-PHI exfiltrateable and available without their consent. As a result of Planned Parenthood's conduct, unauthorized persons did in fact access Plaintiff's and Class members' highly sensitive and confidential e-PHI, in which Plaintiff and

Class members had a reasonable expectation of privacy.

X. PLANNED PARENTHOOD'S PATIENTS HAVE A REASONABLE EXPECTATION OF PRIVACY

114. Plaintiff and Class members have a reasonable expectation of privacy in their intimate health data, which Planned Parenthood collected, stored, and disclosed to unauthorized third parties.

115. It is woefully ironic that Planned Parenthood, an organizational network of affiliates that prides itself on protecting and advocating for the right to privacy and reproductive rights enshrined in the U.S. and California Constitutions by affording patients reproductive healthcare access has allowed itself to be susceptible to the data breach that exposed the highly sensitive and confidential e-PHI of hundreds of thousands patients, including some of the most intimate details of their private lives.

116. Plaintiff and Class members have a reasonable expectation of privacy in their highly sensitive and confidential e-PHI, which Planned Parenthood collected, stored, and disclosed. This expectation of privacy is deeply enshrined in California's Constitution.

117. Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness***, and privacy***." Art. I., Sec. 1, Cal. Const (emphasis added).

118. The phrase "and privacy" was added in 1972 after voters approved a legislative constitutional amendment designated as Proposition 11. Critically, the argument in favor of Proposition 11 reveals that the legislative intent was to curb businesses' control over the unauthorized collection and use of consumers' personal information, stating in relevant part:

> The right of privacy is the right to be left alone . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us.

> **Fundamental to our privacy is the ability to control circulation of personal information.** This is essential to social relationships and personal freedom. The proliferation of government and business records over which we have no control limits our ability to control our personal lives. Often we do not know that these records even exist and we are certainly unable to determine who has access to them.[4]

(emphasis added).

119. Consistent with this language, an abundance of studies examining the collection of consumers' personal data confirms that the surreptitious unauthorized disclosure of highly sensitive and confidential e-PHI from hundreds of thousands of individuals, as Planned Parenthood has done here, violates expectations of privacy that have been established as general social norms.

120. Privacy polls and studies uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' personal data.

121. Surveys consistently show that individuals care about the security and privacy of their e-PHI. In 2013, the *Office of the National Coordinator for Health Information Technology* found that 7 out of 10 individuals are concerned about the privacy of their medical records. The same study found that 3 out of 4 individuals are concerned about the security of their medical records.

122. Likewise, a *Gallup* survey found that 78%of adults believe that it is very important that their medical records be kept confidential, and a majority of respondents believe no one should be permitted to see their records without consent.

123. A recent study by *Consumer Reports* shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before sharing their data and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.

124. Consistent with these expectations, Plaintiff and Class members have taken steps

[4] Ballot Pamp., Proposed Amends. to Cal. Const. with arguments to voters, Gen. Elec. (Nov. 7, 1972) at 27.

specifically to ensure the confidentiality of their medical information and treatment at Planned Parenthood, including not disclosing this information to others and even obscuring the specific treatment on insurance records.

125. Despite Plaintiff and Class members expectation of privacy, Planned Parenthood has failed to obtain adequate authorization and data security practices in connection with its data collection practices and the unauthorized disclosure that occurred. This constitutes a violation of Plaintiff's and Class members' privacy interests, including those explicitly enshrined in the California Constitution.

CLASS ACTION ALLEGATIONS

126. Pursuant to California Code of Civil Procedure § 382, Plaintiff seeks to represent a class defined as follows:

> All persons in the United States whose e-PHI was compromised in the data breach that was made public by Planned Parenthood in November 2021. (the "**Nationwide Class**").

127. Excluded from the Nationwide Class are Defendants and its subsidiaries and affiliates; all employees of Defendants and its subsidiaries and affiliates; all persons who make a timely election to be excluded from the Nationwide Class; Plaintiff's counsel and Planned Parenthood's counsel and members of their immediate families; government entities; and the judge to whom this case is assigned, including his/her immediate family and court staff.

128. Plaintiff reserves the right to modify, expand or amend the above Class definitions or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

CALIFORNIA SUBCLASS

129. Pursuant to California Code of Civil Procedure § 382, Plaintiff seeks to represent a California Subclass defined as follows:

> All persons in the state of California whose e-PHI were compromised in the data breach that was made public by Planned Parenthood in November 2021. (the "**California Subclass**").

130. Excluded from the California Subclass are Defendants and its subsidiaries and affiliates; all employees of Defendants and its subsidiaries and affiliates; all persons who make a timely election to be excluded from the California Class; Plaintiff's counsel and Planned Parenthood's counsel and members of their immediate families; government entities; and the judge to whom this case is assigned, including his/her immediate family and court staff.

131. Plaintiff reserves the right to modify, expand or amend the above Subclass definitions or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

132. **Numerosity:** The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiff is informed and believes that there are likely at least 400,000 members of the Class according to news reports, the precise number of Class members is unknown to Plaintiff. Class members may be identified through objective means including Planned Parenthood's own patient records. Class members may be notified of the pendency of this action by recognized, court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

133. **Commonality and Predominance:** This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

a. Whether Defendants owed a duty to Plaintiff and Class members to secure and safeguard their e-PHI;

b. Whether Defendants failed to use reasonable care and reasonable methods to secure and safeguard Plaintiff's and Class members' e-PHI;

c. Whether Defendants properly implemented security measures as required by HIPAA or any other laws or industry standards to protect Plaintiff's and Class members' e-PHI from unauthorized access, capture, dissemination and misuse;

d. Whether Plaintiff and members of the Class were injured and suffered damages and ascertainable losses as a result of Defendants' actions or failure to act;

e. Whether Defendants engaged in active misfeasance and misconduct alleged

herein;

f. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Defendants' failure to provide adequate security proximately caused Plaintiff's and Class members' injuries; and

h. Whether Plaintiff and Class members are entitled to declaratory and injunctive relief.

134. **Typicality:** Plaintiff is a member of the Class. Plaintiff's claims are typical of the claims of all Class members because Plaintiff, like other Class members, suffered theft of her e-PHI in the data breach.

135. **Adequacy of Representation:** Plaintiff is an adequate Class representative because she is a member of the Class and her interests do not conflict with the interests of other Class members that she seeks to represent. Plaintiff is committed to pursuing this matter for the Class with the Class's collective best interest in mind. Plaintiff has retained counsel competent and experienced in complex class action litigation of this type and Plaintiff intends to prosecute this action vigorously. Plaintiff, and her counsel, will fairly and adequately protect the Class's interests.

136. **Predominance and Superiority:** As described above, common issues of law or fact predominate over individual issues. Resolution of those common issues in Plaintiff's case will also resolve them for the Class's claims. In addition, a class action is superior to any other available means for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Planned Parenthood, so it would be impracticable for members of the Class to individually seek redress for Planned Parenthood's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the

benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

137. This class action is also properly brought and should be maintained as a class action because Plaintiff seeks injunctive relief on behalf of each Class on grounds generally applicable to each Class. Certification is appropriate because Defendants have acted or refused to act in a manner that applies generally to the injunctive Class (i.e., Defendants failed to reasonably protect Plaintiff's and Class Members' e-phi from unauthorized third-party hackers). Thus, any injunctive relief or declaratory relief would benefit the Class as a whole.

138. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

CALIFORNIA LAW APPLIES TO THE ENTIRE CLASS

139. California's substantive laws apply to every member of the Class, regardless of where in the United States the Class member resides.

140. California's substantive laws may be constitutionally applied to the claims of Plaintiff and the Class under the Due Process Clause, 14th Amend. § 1, and the Full Faith and Credit Clause, Art. IV § 1 of the U.S. Constitution. California has significant contacts, or significant aggregation of contacts, to the claims asserted by Plaintiff and all Class members, thereby creating state interests that ensure that the choice of California state law is not arbitrary or unfair.

141. PPLA is incorporated in California, its principal place of business is located in California. PPLA also owns property and conducts substantial business in California, and therefore California has an interest in regulating Planned Parenthood's conduct under its laws. PPLA's decision to reside in California and avail itself of California's laws, and to engage in the challenged conduct from and emanating out of California, renders the application of California law to the claims herein constitutionally permissible.

142. California is also the state from which Planned Parenthood's alleged misconduct emanated. This conduct similarly injured and affected Plaintiff and all other Class members.

143. The application of California laws to the Class is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiff and the proposed Class and Subclass, and California has a greater interest in applying its laws here than any other interested state.

CLAIMS FOR RELIEF

COUNT I

NEGLIGENCE

(On Behalf of the Nationwide Class)

144. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

145. Planned Parenthood is a provider of reproductive healthcare services whose patients, including Plaintiff and Class members, entrust them with highly sensitive and confidential e-PHI in connection with these services.

146. Given the highly sensitive nature of e-PHI and likelihood of harm resulting from its unauthorized access, acquisition, use, or disclosure, multiple statutes, regulations, and guidelines, in addition to the common law, impose a duty on Planned Parenthood to protect this information.

147. For example, the HIPAA Security Rule requires Planned Parenthood to: (a) ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit; (b) proactively identify and protect against reasonably anticipated threats to the security or integrity of the information; (c) protect against reasonably anticipated, impermissible uses or disclosures; (d) put in place the required administrative, physical and technical safeguards; (e) implement policies and procedures to prevent, detect, contain, and correct security violations; (f) effectively train their workforce regarding the proper handling of e-PHI; and (g) designate individual security and privacy officers to ensure compliance.

148. Planned Parenthood also had a duty to use reasonable data security measures under several state and federal laws, including § 5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice

of failing to use reasonable measures to protect consumer data.

149. Planned Parenthood owed a duty of care to Plaintiff and Class members to provide data security consistent with the various statutory requirements, regulations, and other notices described above.

150. Accordingly, Planned Parenthood owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their highly sensitive and confidential e-PHI by, among other things: (a) maintaining adequate security systems to ensure that Plaintiff's and Class members' highly sensitive and confidential e-PHI was adequately secured and protected; (b) implementing processes that would detect a breach of Planned Parenthood's systems in a timely manner; and (c) timely notifying patients, including Plaintiff and Class members, that their highly sensitive and confidential e-PHI had been accessed, acquired, used, or disclosed as a result of a data breach so that Plaintiff and Class members could protect themselves from identify theft by transferring their records to a different provider who maintained adequate security controls, obtaining credit and/or identify theft monitoring protection, canceling or changing their bank account and/or debit or credit card information, and/or taking other appropriate precautions.

151. Planned Parenthood's duty of care arose as a result of, among other things, the special relationship that existed between Planned Parenthood and its patients. Planned Parenthood was the only party in a position to ensure that its systems were sufficient to protect against the foreseeable risk that a data breach could occur, which would result in substantial harm to consumers.

152. Planned Parenthood was subject to an "independent duty" untethered to any contract between Plaintiff and Class members and Planned Parenthood.

153. Planned Parenthood breached their duty to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' highly sensitive and confidential e-PHI by failing to adopt, implement, and maintain adequate security measures.

154. For example, Planned Parenthood failed to implement appropriate systems to detect a breach of their systems. Planned Parenthood negligently failed to abide by the HIPAA Security Rule, among other guidelines and regulations, by failing to protect against anticipated threats to

the security or integrity of Plaintiff's and Class members' highly sensitive and confidential e-PHI, and any reasonably anticipated impermissible uses or disclosures of their highly sensitive and confidential e-PHI.

155. Planned Parenthood also breached their duty to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' highly sensitive and confidential e-PHI by failing to timely notify Plaintiff and Class members that their highly sensitive and confidential e-PHI had been accessed by unauthorized third parties.

156. Planned Parenthood's failure to comply with industry regulations such as HIPAA further evidence their negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' highly sensitive and confidential e-PHI.

157. It was foreseeable to Planned Parenthood that a failure to use reasonable measures to protect its patients' highly sensitive and confidential e-PHI could result in injury to its patients.

158. Actual and attempted breaches of data security were reasonably foreseeable to Planned Parenthood given that other PPFA affiliates had recently been breached before as well as the known frequency of data breaches and various warnings from industry experts.

159. The injuries and harm suffered by Plaintiff and Class members as a result of having their highly sensitive and confidential e-PHI accessed, viewed, acquired, used, or disclosed without authorization was the reasonably foreseeable result of Planned Parenthood's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' highly sensitive and confidential e-PHI. Planned Parenthood knew or should have known that the systems and technologies used for storing Plaintiff's and Class members' highly sensitive and confidential e-PHI allowed that information to be accessed, acquired, used, or disclosed by unauthorized third parties. But for Planned Parenthood's wrongful and negligent breach of duties owed to Plaintiff and Class members, the injuries alleged herein would not have occurred.

160. In connection with the conduct described above, Planned Parenthood acted wantonly, recklessly, and with complete disregard for the consequences Plaintiff and Class members would suffer if their highly sensitive and confidential e-PHI was accessed by unauthorized third parties.

161. In addition to Planned Parenthood's common law duty to exercise reasonable care in securing Plaintiff's and Class members' data, several statutes independently imposed a duty on Planned Parenthood to safeguard highly sensitive e-PHI. Planned Parenthood's violation of these statutory duties, as described below, each independently provides an evidentiary presumption to support Plaintiff's and Class members' negligence claim as negligence *per se*.

HIPAA

162. As alleged above, the HIPAA Security Rule requires Planned Parenthood to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting highly sensitive and confidential e-PHI, which Planned Parenthood negligently failed to implement.

163. The HIPAA Security Rule also requires Planned Parenthood to protect against reasonably anticipated threats to the security or integrity of e-PHI and protect against reasonably anticipated impermissible uses or disclosures, which Planned Parenthood negligently failed to do. *See* 45 C.F.R. Part 160 and Part 164, Subpart A and C.

164. Planned Parenthood's failure to secure Plaintiff's and Class members' e-PHI and to notify them that such information had been accessed by unauthorized third parties violated at least the following HIPAA regulations:

a. The HIPAA Privacy and Security Rule 45 C.F.R. § 160 and 45 C.F.R. § 164, Subpart A, C, and E
    i. 45 C.F.R. § 164.306
    ii. 45 C.F.R. § 164.308
    iii. 45 C.F.R. § 164.312
    iv. 45 C.F.R. § 164.314
    v. 45 C.F.R. § 164.502
    vi. 45 C.F.R. § 164.530

165. The harm that has occurred is the type of harm that HIPAA was intended to guard against, namely, the disclosure of patients' sensitive patient information, including e-PHI.

166. Plaintiff and Class members are within the class of persons that the HIPAA Privacy

and Security Rule were intended to protect, because the HIPAA Privacy and Security rule were expressly designed to protect sensitive patient information.

167. Planned Parenthood had a duty to Plaintiff and Class members to implement and maintain reasonable security procedures and practices under HIPAA to safeguard Plaintiff's and Class members' highly sensitive and confidential e-PHI.

168. Planned Parenthood breached their duties to Plaintiff and Class members under the HIPAA, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' highly sensitive and confidential e-PHI.

169. Planned Parenthood's violations of HIPAA and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

FTC Act, 15 U.S.C. § 45

170. As alleged above, pursuant to the FTC Act, 15 U.S.C. § 45, Planned Parenthood had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' highly sensitive and confidential e-PHI.

171. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the failure to use reasonable measures to protect highly sensitive and confidential e-PHI. The FTC publications and orders described above also form part of the basis of Planned Parenthood's duty.

172. Planned Parenthood violated Section 5 of the FTC Act by failing to use reasonable measures to protect highly sensitive and confidential e-PHI and comply with applicable industry standards, including the FTC Act, as described in detail herein. Planned Parenthood's conduct was particularly unreasonable given the nature and amount of e-PHI it collected and stored and the foreseeable consequences of a data breach, including specifically, as described herein, the damages that would result to consumers.

173. The harm that has occurred is the type of harm the FTC Act was intended to guard against, namely harm to consumers as a result of unfair practices in commerce.

174. Indeed, the FTC has pursued numerous enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and

deceptive practices, caused the same harm as that suffered by Plaintiff and Class members.

175. Planned Parenthood had a duty to Plaintiff and Class members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class members' highly sensitive and confidential e-PHI.

176. Planned Parenthood breached their duties to Plaintiff and Class members under the FTC Act, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' highly sensitive and confidential e-PHI.

177. Planned Parenthood's violations of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

California's Confidentiality of Medical Information Act

Cal. Civ. Code § 56, *et seq*.

178. Under the CMIA, "[a]n electronic health record system or electronic medical record system shall do the following: (A) Protect and preserve the integrity of electronic medical information; [and] (B) Automatically record and preserve any change or deletion of any electronically stored medical information. The record of any change or deletion shall include the identity of the person who accessed and changed the medical information, the date and time the medical information was accessed, and the change that was made to the medical information." Cal. Civ. Code § 56.101(b)(1)(A) – (B).

179. Planned Parenthood violated the CMIA by negligently maintaining, preserving, and storing Plaintiff's and Class members' medical information inasmuch as it did not implement adequate security protocols to prevent unauthorized access to medical information, maintain an adequate electronic security system to prevent data breaches, or employ industry standard and commercially viable measures to mitigate the risks of any data the risks of any data breach or otherwise comply with HIPAA data security requirements.

180. Planned Parenthood failed to protect and preserve the integrity of electronic medical information and automatically record and preserve any change or deletion of any electronically stored medical information.

181. Plaintiff and Class members are within the class of persons the CMIA is intended

to protect against, namely, patients of health care providers.

182. The harm that has occurred is the type of harm the CMIA was intended to guard against, namely protecting and preserving the integrity of electronic medical information.

183. As a direct and proximate result of Planned Parenthood's negligence, Plaintiff's and Class members' medical information was accessed and exfiltrated by an unauthorized third party and they were injured as a result.

184. The injury and harm suffered by Plaintiff and Class members was a reasonably foreseeable result of Planned Parenthood's breach of its duties. Planned Parenthood knew or should have known that the breach of its duties would cause Plaintiff and Class members to suffer the foreseeable harms associated with the exposure of their medical information.

185. Planned Parenthood's violations of the CMIA constitutes negligence *per se*.

186. As a direct and proximate result of Planned Parenthood's negligence, including violations of HIPAA, the FTC Act, and the CMIA constituting negligence *per se*, Plaintiff and Class members sustained damages, including violation of their privacy interest and emotional distress, as alleged herein. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the data breach.

187. As a result of Defendants' negligence, Plaintiff and Class members are also entitled to injunctive relief requiring Planned Parenthood to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to Plaintiff and all Class members.

COUNT II

BREACH OF CONTRACT

(On behalf of the Nationwide Class)

188. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

189. Planned Parenthood expressly promised to safeguard Plaintiff's and Class members' highly sensitive and confidential e-PHI in accordance with the applicable state and

federal laws and/or regulations. Additionally, Planned Parenthood promised to abide by their own Privacy Policy, which they provided to patients.

190. This Privacy Policy applied to Plaintiff and Class members who accepted Planned Parenthood's promise and entered into a contract with Planned Parenthood when they entrusted their highly sensitive and confidential e-PHI to Planned Parenthood as part of a transaction for medical goods and services.

191. Plaintiff and Class members fully performed their obligations under their contracts with Defendant, including by providing their highly sensitive and confidential e-PHI and receiving treatment at Planned Parenthood.

192. Planned Parenthood did not hold up their end of the bargain. In entering into such contracts, Planned Parenthood agreed to protect Plaintiff's and Class members' highly sensitive and confidential e-PHI, secure the servers and systems that housed Plaintiff's and Class members' highly sensitive and confidential e-PHI, and to provide timely notice if their highly sensitive and confidential e-PHI was accessed, acquired, used, of disclosed.

193. Planned Parenthood failed on all accounts: they failed to take reasonable steps to protect Plaintiff's and Class members' highly sensitive and confidential e-PHI, secure their servers and systems that stored Plaintiff's and Class members' highly sensitive and confidential e-PHI. Each of these acts constituted a separate breach of the contracts Planned Parenthood entered with Plaintiff and Class members.

194. Plaintiff and Class members would not have entrusted Planned Parenthood with their highly sensitive and confidential e-PHI in the absence of the contract between them and Defendant, obligating Planned Parenthood to keep this information secure and provide timely notice in the event of a breach.[5]

195. As a direct and proximate result of Planned Parenthood's breaches of their contracts, Plaintiff and Class members sustained damages as alleged herein, including when they

[5] This is consistent with most consumer attitudes. A recent study by CynergisTek, a leading cybersecurity firm, found that 70 percent of individuals would be likely to cut ties with a healthcare provider who was not properly securing their personal health data.

received services that did not include reasonable security measures sufficient to protect Plaintiff's and Class members' highly sensitive and confidential e-PHI, despite Planned Parenthood's promise that it would do so. Plaintiff and Class members would not have usedPlanned Parenthood's services had they known these representations were false.

196. Plaintiff and Class members are entitled to compensatory and consequential damages as a result of Planned Parenthood's breach of contract.

COUNT III

BREACH OF IMPLIED CONTRACT

(On behalf of the Nationwide Class)

197. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

198. When Plaintiff and Class members provided their highly sensitive and confidential e-PHI to Planned Parenthood in exchange for Planned Parenthood's services, they entered into implied contracts with Planned Parenthood under which Defendants agreed to take reasonable steps to protect their highly sensitive and confidential e-PHI.

199. Planned Parenthood solicited and invited Plaintiff and Class members to provide their highly sensitive and confidential e-PHI as part of Planned Parenthood's regular business practices. Plaintiff and Class members accepted Planned Parenthood's offers and provided their highly sensitive and confidential e-PHI to Defendant.

200. When entering into the implied contracts, Plaintiff and Class members reasonably believed and expected that Planned Parenthood's data security practices complied with relevant laws, regulations, and industry standards.

201. When entering into the implied contracts, Plaintiff and Class members reasonably believed that Planned Parenthood would safeguard and protect their highly sensitive and confidential e-PHI and that Planned Parenthood would use part of the funds received from Plaintiff and Class members to pay for adequate and reasonable data security practices. Planned Parenthood failed to do so.

202. Plaintiff and Class members would not have provided their highly sensitive and

confidential e-PHI to Planned Parenthood in the absence of Planned Parenthood's implied promise to keep their highly sensitive and confidential e-PHI reasonably secure.

203. Plaintiff and Class members fully performed their obligations under the implied contracts by paying money to Planned Parenthood.

204. Planned Parenthood breached its implied contracts with Plaintiff and Class members by failing to safeguard and protect their highly sensitive and confidential e-PHI.

205. As a direct and proximate result of Planned Parenthood's breaches of implied contracts, Plaintiff and Class members sustained damages as alleged herein, including when they received services that did not include reasonable security measures sufficient to protect Plaintiff's and Class members' highly sensitive and confidential e-PHI, despite Planned Parenthood's promise that it would do so. Plaintiff and Class members would not have used Planned Parenthood's services had they known these representations were false.

206. Plaintiff and Class members are also entitled to injunctive relief requiring Planned Parenthood to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class members.

COUNT IV

UNJUST ENRICHMENT

(On behalf of the Nationwide Class)

207. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

208. Plaintiff and Class members conferred a monetary benefit upon Planned Parenthood when Planned Parenthood was paid for services received by Plaintiff and Class members.

209. Planned Parenthood appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class members. Planned Parenthood also benefited from the receipt of Plaintiff's and Class members' highly sensitive and confidential e-PHI.

210. The funds paid to Planned Parenthood were supposed to be used by Planned

Parenthood, in part, to pay for adequate data privacy infrastructure, practices, and procedures.

211. As a result of Planned Parenthood's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between what they paid for, Planned Parenthood's medical goods/services made with adequate data privacy and security practices and procedures, and what they received, Planned Parenthood's medical goods/services without adequate data privacy and security practices and procedures.

212. Under principals of equity and good conscience, Planned Parenthood should not be permitted to retain the money belonging to Plaintiff and Class members or other third parties because Planned Parenthood failed to implement, or adequately implement, the data privacy and security practices that were otherwise mandated by federal, state, and local laws and industry standards.

213. Planned Parenthood should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds received by it as a result of the conduct and data breach alleged herein.

COUNT V

COMMON LAW INVASION OF PRIVACY – INTRUSION UPON SECLUSION

(On behalf of the Nationwide Class)

214. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

215. Plaintiff asserts claims for intrusion upon seclusion must plead (1) that the defendant intentionally intruded into a matter as to which plaintiff had a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

216. There is no area where there is more of a reasonable expectation of privacy than in the area of reproductive healthcare, which are the types of services Planned Parenthood provides.

217. Planned Parenthood intentionally intruded upon the solitude, seclusion and private affairs of Plaintiff and Class members by intentionally configuring their systems in such a way that left them vulnerable to malware/ransomware attack, thus permitting unauthorized access to their systems, which compromised Plaintiff's and Class members' highly sensitive and

confidential e-PHI. Only Planned Parenthood had control over its systems.

218. Planned Parenthood's conduct is especially egregious and offensive as they failed to have any adequate security measures in place to prevent, track, or detect in a timely fashion unauthorized access to Plaintiff's and Class members' e-PHI.

219. At all times, Planned Parenthood was aware that Plaintiff's and Class members' highly sensitive and confidential e-PHI in their possession contained highly sensitive medical information, including patient name, and one or more of the following: dates of birth, addresses, insurance identification numbers, and clinical data (such as diagnosis, treatment, or prescription information).

220. Plaintiff and Class members have a reasonable expectation in their e-PHI, which contains highly sensitive medical information.

221. Planned Parenthood intentionally configured their systems in such a way that stored Plaintiff's and Class Members' highly sensitive and confidential e-PHI to be left vulnerable to malware/ransomware attack without regard for Plaintiff's and Class members' privacy interests.

222. The disclosure of the highly sensitive and confidential e-PHI of 400,000 patients, was highly offensive to Plaintiff and Class members because it violated expectations of privacy that have been established by general social norms, including by granting access to information and data that is private and would not otherwise be disclosed.

223. Surveys consistently show that individuals care about the security and privacy of their highly sensitive and confidential e-PHI. In 2013, the *Office of the National Coordinator for Health Information Technology* found that 7 out of 10 individuals are concerned about the privacy of their medical records. The same study found that 3 out of 4 individuals are concerned about the security of their medical records. Likewise, a *Gallup* survey found that 78%of adults believe that it is very important that their medical records be kept confidential, and a majority of respondents believe no one should be permitted to see their records without consent. Plaintiff and Class members acted consistent with these polls and surveys by safeguarding their medical information, including the ePHI exfiltrated and stolen in the data breach.

224. Planned Parenthood's conduct would be highly offensive to a reasonable person in

that it violated statutory and regulatory protections designed to protect highly sensitive medical information, in addition to social norms. Planned Parenthood's conduct would be especially egregious to a reasonable person as Planned Parenthood publicly disclosed Plaintiff's and Class members' highly sensitive and confidential e-PHI without their consent, including to an "unauthorized person," i.e., hackers.

225. As a result of Planned Parenthood's actions, Plaintiff and Class members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

226. Plaintiff and Class members have been damaged as a direct and proximate result of Planned Parenthood's intrusion upon seclusion and are entitled to just compensation.

227. Plaintiff and Class members are entitled to appropriate relief, including compensatory damages for the harm to their privacy, loss of valuable rights and protections, and heightened risk of future invasions of privacy.

COUNT VI

INVASION OF PRIVACY

ART. I, SEC 1 OF THE CALIFORNIA CONSTITUTION

(On behalf of the California Subclass)

228. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

229. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

230. The right to privacy in California's constitution creates a private right of action against private and government entities.

231. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

232. Planned Parenthood violated Plaintiff's and California Subclass members' constitutional right to privacy by collecting, storing, and disclosing (1) e-PHI in which they had a legally protected privacy interest, (2) Plaintiff's and California Subclass members' e-PHI in which they had a reasonable expectation of privacy in, (3) in a manner that was highly offensive to Plaintiff and California Subclass members, would be highly offensive to a reasonable person, and was in egregious violation of social norms.

233. Planned Parenthood have intruded upon Plaintiff's and California Subclass members' legally protected privacy interests, including, *inter alia*: (i) interests in precluding the dissemination or misuse of sensitive and confidential personal—the e-PHI; and (ii) interests in making intimate personal healthcare decisions or conducting personal activities without observation, intrusion, or interference.

234. The highly sensitive and confidential e-PHI, which Planned Parenthood stored, monitored, collected, and disclosed without Plaintiff's and California Subclass members' authorization and/or consent included, *inter alia*, patient names, dates of birth, addresses, insurance identification numbers, and clinical data (such as diagnosis, treatment, or prescription information).

235. Plaintiff and California Subclass members had a legally protected informational privacy interest in the confidential and sensitive e-PHI involved as well as a privacy interest in conducting their personal healthcare decisions and activities without intrusion, interference, or disclosure.

236. Planned Parenthood's actions constituted a serious invasion of privacy that would be highly offensive to a reasonable person in that: (i) the invasion occurred within a zone of privacy protected by the California Constitution, namely the misuse of information gathered for an improper purpose; and (ii) the invasion deprived Plaintiff and California Subclass members of the ability to control the circulation of their highly sensitive and confidential e-PHI, which is considered fundamental to the right to privacy.

237. Plaintiff and California Subclass members had a reasonable expectation of privacy in that: (i) Planned Parenthood's invasion of privacy occurred as a result of Planned Parenthood's

security practices including the collecting, storage, and unauthorized disclosure of highly sensitive and confidential e-PHI; (ii) Plaintiff and California Subclass members did not consent or otherwise authorize Planned Parenthood to disclosure their highly sensitive and confidential e-PHI; and (iii) Plaintiff and California Subclass members could not reasonably expect Planned Parenthood would commit acts in violation of laws protecting privacy.

238. As a result of Planned Parenthood's actions, Plaintiff and California Subclass members have been damaged as a direct and proximate result of Planned Parenthood's invasion of their privacy and are entitled to just compensation.

239. Plaintiff and California Subclass members suffered actual and concrete injury as a result of Planned Parenthood's violations of their privacy interests. Plaintiff and California Subclass members are entitled to appropriate relief, including damages to compensate them for the harm to their privacy interests, loss of valuable rights and protections, heightened risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Defendants' invasions.

240. Plaintiff and the California Subclass seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and California Subclass members for the harm to their privacy interests as well as disgorgement of profits made by Planned Parenthood as a result of its intrusions upon Plaintiff's and California Subclass members' privacy.

COUNT VII

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW

Cal. Bus. & Prof. Code § 17200, *et seq.*

(On Behalf of the California Subclass)

241. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

242. Planned Parenthood is a "person" as defined by Cal. Bus. & Prof. Code §17201.

243. Planned Parenthood violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

244. Planned Parenthood's business acts and practices are "unlawful" under the Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 *et. seq.* ("UCL"), because, as alleged above, Planned Parenthood violated the California common law, California Constitution, and the other state and federal statutes and causes of action described herein.

245. Planned Parenthood's business acts and practices are "unfair" under the UCL, because, as alleged above, California has a strong public policy of protecting consumers' privacy interests, including protecting consumers' personal data, including highly sensitive and confidential e-PHI. Planned Parenthood violated this public policy by, among other things, surreptitiously collecting, storing, disclosing, and otherwise misusing Plaintiff's and California Subclass members' highly sensitive and confidential e-PHI without Plaintiff's and California Subclass members' consent. Planned Parenthood further engaged in unfair business practices because it made material misrepresentations and omissions concerning the information that Planned Parenthood assured patients it would protect their highly sensitive and confidential e-PHI, which deceived and misled patients. Planned Parenthood's conduct violates the policies of the statutes referenced herein.

246. Planned Parenthood's business acts and practices are also "unfair" in that they are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to consumers. The gravity of the harm of Planned Parenthood's collecting, storing, disclosing, and otherwise misusing Plaintiff's and California Subclass members' highly sensitive and confidential e-PHI is significant, and there is no corresponding benefit resulting from such conduct. Finally, because Plaintiff and California Subclass members were completely unaware of Planned Parenthood's conduct, they could not have possibly avoided the harm.

247. Planned Parenthood's business acts and practices are also "fraudulent" within the meaning of the UCL. Planned Parenthood misrepresented that it maintained sufficient data security measures and systems to protect Plaintiff's and California Subclass members' e-PHI. Planned Parenthood never disclosed that these practices were severely deficient.

248. Planned Parenthood's unlawful, unfair, and deceptive acts and practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to

protect Plaintiff's and California Subclass members' e-PHI, which was a direct and proximate cause of the data breach and omitting, suppressing, and concealing the material fact of that failure;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following well-publicized cybersecurity incidents, which was a direct and proximate cause of the data breach and omitting, suppressing, and concealing the material fact of that failure;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' e-PHI, including duties imposed by the FTC Act, HIPAA, and CMIA which was a direct and proximate cause of the data breach and omitting, suppressing, and concealing the material fact of that failure;

(d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and California Subclass members' e-PHI, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' e-PHI, including duties imposed by the FTC Act, HIPAA, and CMIA;

(f) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and California Subclass members' e-PHI; and

(g) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' e-PHI, including duties imposed by the FTC Act, HIPAA, and the CMIA.

249. Planned Parenthood's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Planned Parenthood's data security and ability to protect the confidentiality of consumers' highly sensitive and confidential

e-PHI.

250. As a direct and proximate result of Planned Parenthood's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass members were injured and lost money or property, i.e., costs to be spent for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their highly sensitive and confidential e-PHI; and an increased, imminent risk of fraud and identity theft.

251. Planned Parenthood's violations were, and are, willful, deceptive, unfair, and unconscionable.

252. Plaintiff and California Subclass members have lost money and property as a result of Planned Parenthood's conduct in violation of the UCL, as stated in herein and above. Health data, such as the e-PHI collected by Planned Parenthood, objectively has value. For instance, Pfizer annually pays approximately $12 million to purchase health data from various sources.

253. Consumers and patients, including Plaintiff and California Subclass members also value their health data. According to the annual Financial Trust Index Survey, conducted by *the University of Chicago's Booth School of Business and Northwestern University's Kellogg School of Management*, which interviewed more than 1,000 Americans, 93%would not share their health data with a digital platform for free. Half of the survey respondents would only share their data for $100,000 or more, and 22% would only share their data if they received between $1,000 and $100,000.

254. By deceptively storing, collecting, and disclosing this highly sensitive and confidential e-PHI, Planned Parenthood has taken money or property from Plaintiff and California Subclass members.

255. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including compensatory damages; restitution; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

COUNT VIII

VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL

INFORMATION ACT,

Cal. Civ. Code § 56, *et seq.*

(On Behalf of the California Subclass)

256. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

257. Under the CMIA, "medical information" is defined as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. "Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity." Cal. Civ. Code § 56.05(j). Plaintiff's and California Subclass members' highly sensitive and confidential e-PHI constitutes "medical information" under the CMIA because it contained individually identifiable information in the possession or derived from Planned Parenthood.

258. Under the CMIA, "provider of health care" means "any person licensed or certified pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code; any person licensed pursuant to the Osteopathic Initiative Act or the Chiropractic Initiative Act; any person certified pursuant to Division 2.5 (commencing with Section 1797) of the Health and Safety Code; any clinic, health dispensary, or health facility licensed pursuant to Division 2 (commencing with Section 1200) of the Health and Safety Code." Cal. Civ. Code § 56.05(m).

259. Planned Parenthood as a "provider of health care" is subject to the CMIA, because it is a "business organized for the purpose of maintaining medical information, as defined in subdivision (j) of Section 56.05, in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis and treatment of the individual, shall be deemed to be a provider of health care subject to the requirements of this

part." Cal. Civ. Code § 56.06(a). As such, Planned Parenthood is subject to the penalties for improper use and disclosure of medical information prescribed in this part." Cal. Civ. Code § 56.06(e).

260. Under the CMIA, "patient" means "any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains. Cal. Civ. Code § 56.05(k)." Plaintiff and California Subclass members are "patients" under the CMIA.

261. Under the CMIA, "authorized recipient" means "any person who is authorized to receive medical information pursuant to Section 56.10 or 56.20. Cal. Civ. Code § 56.05(b)." Planned Parenthood is a "authorized recipient" under the CMIA.

262. Planned Parenthood stored in electronic form on its computer system Plaintiff's and California Subclass members' "medical information" as defined by Cal. Civ. Code § 56.05(j).

263. Planned Parenthood's systems were designed, in part, to make medical information available to Planned Parenthood so it could store, access, and manage patients' medical information, including but not limited to diagnosing, treating, or managing patients' medical conditions.

264. Under the CMIA, "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization, except as provided in subdivision (b) or (c)." Cal. Civ. Code § 56.10(a).

265. Planned Parenthood violated Cal. Civ. Code § 56.10(a) as Plaintiff and California Subclass members did not provide Planned Parenthood authorization nor was Planned Parenthood otherwise authorized to disclose Plaintiff's or California Subclass members' medical information to an unauthorized third-party.

266. As a direct and proximate result of Planned Parenthood's violation of Cal. Civ. Code Section 56.10(a), Plaintiff's and California Subclass members' medical information was viewed by an unauthorized third party.

267. Planned Parenthood's unauthorized disclosures of Plaintiff's and California

Subclass members' medical information has caused injury to Plaintiff and California Subclass members.

268. In addition, Cal. Civil Code Section 56.101, subdivision (a), requires that every provider of health care "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein."

269. Further, "[a]n electronic health record system or electronic medical record system shall do the following:(A) Protect and preserve the integrity of electronic medical information; [and] (B) Automatically record and preserve any change or deletion of any electronically stored medical information. The record of any change or deletion shall include the identity of the person who accessed and changed the medical information, the date and time the medical information was accessed, and the change that was made to the medical information." Cal. Civ. Code § 56.101(b)(1)(A) – (B).

270. Planned Parenthood failed to maintain, preserve, and store medical information in a manner that preserves the confidentiality of the information contained therein because it disclosed to third parties Plaintiff's and California Subclass members' highly sensitive and confidential e-PHI without consent.

271. As described throughout this Complaint, Planned Parenthood also violated Cal. Civ. Code § 56.101(a) by negligently maintaining, preserving, and storing Plaintiff's and California Subclass members' medical information inasmuch as it did not implement adequate security protocols to prevent unauthorized access to medical information, maintain an adequate electronic security system to prevent data breaches, or employ industry standard and commercially viable measures to mitigate the risks of any data the risks of any data breach or otherwise comply with HIPAA data security requirements.

272. Planned Parenthood failed to protect and preserve the integrity of electronic medical information and automatically record and preserve any change or deletion of any electronically stored medical information.

273. As a direct and proximate result of Planned Parenthood's violation of Cal. Civ.

Code Section 56.101(a), Plaintiff's and California Subclass members' medical information was viewed by an unauthorized third party.

274. Planned Parenthood's negligent maintenance, preservation, and storage of Plaintiff's and California Subclass members' medical information has caused injury to Plaintiff and California Subclass members.

275. Accordingly, Plaintiff and California Subclass members are entitled to: (1) nominal damages of $1,000 per violation; (2) actual damages, in an amount to be determined at trial; (3) statutory damages pursuant to 56.36(c); (4) punitive damages pursuant to Cal. Civ. Code Section 56.35; and (5) reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT IX

REQUEST FOR RELIEF UNDER THE DECLARATORY JUDGMENT ACT

28 U.S.C. § 2201, *et seq.*

(On Behalf of the Nationwide Class)

276. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

277. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

278. An actual controversy has arisen in the wake of the data breach regarding Planned Parenthood's present and prospective common law and statutory duties to reasonably safeguard its patients' highly sensitive and confidential e-PHI and whether Planned Parenthood is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches. Plaintiff alleges that Planned Parenthood's data security practices remain inadequate.

279. Plaintiff and Class members continue to suffer injury as a result of the compromise of their highly sensitive and confidential e-PHI and remain at imminent risk that further compromises of their personal information will occur in the future.

280. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Planned Parenthood continues to owe a legal duty to secure consumers' highly sensitive and confidential e-PHI, to timely notify consumers of any data breach, and to establish and implement data security measures that are adequate to secure its patients' highly sensitive and confidential e-PHI.

281. The Court also should issue corresponding prospective injunctive relief requiring Planned Parenthood to employ adequate security protocols consistent with law and industry standards to protect patients' highly sensitive and confidential e-PHI.

282. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury, for which they lack an adequate legal remedy. The threat of another data breach is real, immediate, and substantial. If another breach at Planned Parenthood occurs, Plaintiff and Class members will not have an adequate remedy at law, because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

283. The hardship to Plaintiff and Class members if an injunction does not issue greatly exceeds the hardship to Planned Parenthood if an injunction is issued. If another data breach occurs at Planned Parenthood, Plaintiff and Class members will likely be subjected to substantial identify theft and other damages. On the other hand, the cost to Planned Parenthood of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Planned Parenthood has a pre-existing legal obligation to employ such measures.

284. Issuance of the requested injunction will serve the public interest by preventing another data breach at Planned Parenthood, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose confidential information would be further compromised.

COUNT X

VIOLATION OF THE CALIFORNIA CONSUMER RECORDS ACT

Cal. Civ. Code § 1798.80 *et seq.*

(On Behalf of the California Subclass)

285. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully

set forth herein.

286. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California [] whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person…" Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonably delay…"

287. The California Consumer Records Act ("CCRA") further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

288. Plaintiff and the California Subclass members are residents of California and are "consumers" within the meaning of California Civil Code § 1798.80(c).

289. Defendants are "business(es)" within the meaning of California Civil Code § 1798.80(a) which includes "a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit."

290. The data breach was a breach of security within the meaning of section 1798.82. The PHI and e-PHI stolen constitutes "personal information" within the meaning of California Civil Code §1798.80.

291. Any person or business that is required to issue a security breach notification under the CCRA shall meet all of the following requirements:

a. The security breach notification shall be written in plain language;

b. The security breach notification shall include, at a minimum, the following information:

i. The name and contact information of the reporting person or

business subject.

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

iii. If the information is possible to determine at the time the notice is provided, then any of the following:

1. The date of the breach;
2. The estimated date of the breach; or
3. The date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

vi. The toll-free telephone number and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

292. In violation of the CCRA, Defendants unreasonably delayed in notifying Plaintiff and members of the California Subclass of the data breach, in which they were aware on or before October 17, 2021.

293. As a result of Defendants' violation of Cal. Civ. Code § 1798.82(b), Plaintiff and California Subclass members were deprived of prompt notice of the data breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection, as well as future costs related to the same. These measures could have prevented some of the damages Plaintiff and California Subclass members have suffered and will suffer because their PHI and e-PHI would have had less value to identity thieves.

294. As a result of Defendants' violation Cal. Civ. Code § 1798.82(b), Plaintiff and California Subclass members suffered incrementally increased damages separate and distinct from

those simply caused by the data breach itself.

295. Plaintiff and California Subclass members seek all remedies available under Cal. Civ. Code § 1798.82(b), including but not limited to the damages suffered by Plaintiff and California Subclass members as alleged above, and equitable relief.

RELIEF REQUESTED

Plaintiff, on behalf of all others similarly situated, requests that the Court enter judgment against Defendants including the following:

A. Determining that this matter may proceed as a class action and certifying the Class asserted herein;

B. Appointing Plaintiff as representative of the applicable Classs and appointing Plaintiff's counsel as Class counsel;

C. An award to Plaintiff and the Class of compensatory, consequential, nominal, statutory, and treble damages as set forth above;

D. Ordering injunctive relief requiring Defendants to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; (iii) provide several years of free credit monitoring and identity theft insurance to all Class members; and (iv) timely notify consumers of any future data breaches;

E. Entering a declaratory judgment stating that Defendants owe a legal duty to secure consumers' e-PHI, to timely notify patients of any data breach, and to establish and implement data security measures that are adequate to secure patients' e-PHI;

F. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

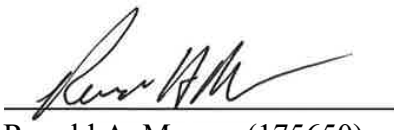
G. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

H. Such other relief as the Court may allow.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Dated: December 23, 2021



Ronald A. Marron (175650)
Alexis M. Wood (270200)
Kas L. Gallucci (288709)
Lilach Halperin (323202)
LAW OFFICES OF RONALD A. MARRON
651 Arroyo Drive
San Diego, CA 92103
Tel: (619) 696-9006
Fax: (619) 564-6665
ron@consumersadvocates.com
alexis@consumersadvocates.com
kas@consumersadvocates.com
lilach@consumersadvocates.com

Christian Levis (pro hac vice forthcoming)
Amanda Fiorilla (pro hac vice forthcoming)
Rachel Isabel Kesten (pro hac vice forthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Fax: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com
rkesten@lowey.com

Anthony M. Christina (pro hac vice forthcoming)
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428 Telephone: (215) 399-4770
Fax: (914) 997-0035
achristina@lowey.com

Attorneys for Plaintiff and the Proposed Class

EXHIBIT A

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

Planned Parenthood®
Care. No matter what.
Planned Parenthood Los Angeles

November 30, 2021

H1202-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Dear Sample:

At Planned Parenthood Los Angeles ("PPLA"), we take our commitment to privacy very seriously, and we work hard to protect our patients' information. We are writing to inform you of an incident involving some of your information. This letter explains the incident, measures we have taken, and some steps you may consider taking in response.

What Happened
On October 17, 2021, we identified suspicious activity on our computer network. We immediately took our systems offline, notified law enforcement, and a third-party cybersecurity firm was engaged to assist in our investigation. The investigation determined that an unauthorized person gained access to our network between October 9, 2021 and October 17, 2021, and exfiltrated some files from our systems during that time.

What Information Was Involved
As soon as we determined what files were involved, we began a review to determine what they contained. On November 4, 2021, we identified files that contained your name and one or more of the following: address, insurance information, date of birth, and clinical information, such as diagnosis, procedure, and/or prescription information.

What You Can Do
At this time, we have no evidence that any information involved in this incident has been used for fraudulent purposes. However, in an abundance of caution, we wanted to notify you of this incident and assure you that we take this very seriously. It is always a good idea to review statements you receive from your health insurer and health care providers. If you see charges for services you did not receive, please call the insurer or provider immediately.

What We Are Doing
We have and will continue to take steps to enhance our existing security measures and to help protect the information in our care, including increasing our network monitoring, engaging an external cybersecurity firm, and hiring additional cybersecurity resources and talent to our team.

For More Information
We deeply regret that this incident occurred and for any concern this may cause you. If you have questions about this incident, please call (866) 665-2966, Monday through Friday from 6 a.m. to 8 p.m. Pacific Time, and Saturday and Sunday from 8 a.m. to 5 p.m. Pacific Time. Callers should provide Engagement Number **B021848** to the operator.

Sincerely,

Kevin Oliver
Compliance Officer

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

Planned Parenthood®
Care. No matter what.
Planned Parenthood Los Angeles

30 de noviembre de 2021

SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Estimado Sample:

En Planned Parenthood de Los Angeles ("PPLA"), tomamos muy en serio nuestro compromiso con la privacidad y trabajamos arduamente para proteger la información de nuestros pacientes. Hoy le escribimos para informarle de un incidente relacionado con parte de su información. Esta carta explica el incidente, las medidas que hemos tomado y algunos pasos que puede considerar tomar como respuesta.

Qué sucedió
El 17 de octubre de 2021, identificamos actividad sospechosa en nuestra red informática. Inmediatamente desconectamos nuestros sistemas, notificamos a la policía y contratamos a una empresa independiente de ciberseguridad para ayudar con nuestra investigación. La investigación determinó que una persona no autorizada obtuvo acceso a nuestra red entre el 9 de octubre de 2021 y el 17 de octubre de 2021, y exfiltró algunos archivos de nuestros sistemas durante ese tiempo.

Qué información estuvo involucrada
Tan pronto como determinamos qué archivos estaban involucrados, comenzamos una revisión para determinar qué contenían. El 4 de noviembre de 2021, identificamos archivos que contenían el nombre de usted y uno o más de los siguientes: dirección, información del seguro, fecha de nacimiento e información clínica, como diagnóstico, procedimiento o información de recetas de medicamentos.

Lo que usted puede hacer
En este momento, no tenemos ninguna evidencia de que la información involucrada en este incidente haya sido utilizada con fines fraudulentos. Sin embargo, como una medida extrema de precaución, quisimos notificarle de este incidente y asegurarle que lo estamos tomando muy en serio. Una buena idea es la de siempre revisar las declaraciones que recibe de su aseguradora de salud y de sus proveedores de atención médica. Si ve cargos por servicios que usted no recibió, llame inmediatamente a la aseguradora o al proveedor.

Lo que estamos haciendo
Estamos tomando los pasos necesarios para mejorar nuestras medidas de seguridad y para ayudar a proteger la información que se encuentra bajo nuestro cuidado, incluido el aumento de nuestro monitoreo de red, la participación de una empresa de ciberseguridad externa y la contratación de recursos y talento de ciberseguridad adicionales para nuestro equipo.

Para más información
Lamentamos profundamente que este incidente haya ocurrido y cualquier preocupación que esto pueda ocasionarle. Si tiene preguntas sobre este incidente, llame al (866) 665-2966, de lunes a viernes, entre las 6:00 a.m. y las 8:00 p.m. y de sabado a domingo entre las 8:00 a.m. y las 5:00 p.m., horario del Pacífico. Al llamar deberá proporcionar su número de participación **B021848** al operador.

Atentamente,

Kevin Oliver
Oficial de Cumplimiento