

1 **CONSUMER WATCHDOG**

2 Jerry Flanagan (SBN: 271272)  
3 jerry@consumerwatchdog.org  
4 Daniel L. Sternberg (SBN: 329799)  
5 danny@consumerwatchdog.org  
6 6330 San Vicente Blvd., Suite 250  
Los Angeles, CA 90048  
Tel: (310) 392-0522  
Fax: (310) 392-8874

7 **WHATLEY KALLAS, LLP**

8 Alan M. Mansfield (of counsel, SBN: 125998)  
9 amansfield@whatleykallas.com  
10 16870 W. Bernardo Dr., Suite 400  
11 San Diego, CA, 92127  
12 Tel: (858) 674-6641  
13 Fax: (855) 274-1888

14 **Attorneys for Plaintiff**

15  
16 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**  
17 **COUNTY OF LOS ANGELES, CENTRAL DISTRICT**

18 JOHN DOE, on behalf of himself and all others  
19 similarly situated and for the benefit of the general  
20 public,

21 Plaintiff,

22 v.

23 CALIFORNIA DEPARTMENT OF PUBLIC  
24 HEALTH; SANDRA SHEWRY, Acting Director  
25 of the California Department of Public Health, in  
26 her official capacity; THRIVE TRIBE  
27 FOUNDATION; EVOLVE HEALTHCARE;  
28 GARY GOLDSTEIN; GOOD HEALTH, INC.  
D/B/A PREMIER PHARMACY SERVICES; and  
DOES 2 through 25, inclusive,

Defendants.

**FILED**  
Superior Court of California  
County of Los Angeles

10/06/2022

Sherri R. Carter, Executive Officer / Clerk of Court

By:           K. Martinez           Deputy

Case No. 20STCV32364

**FIRST AMENDED CLASS ACTION  
COMPLAINT**

- (1) Information Practices Act of 1977
- (2) AIDS Public Health Records Confidentiality Act
- (3) Confidentiality of Medical Information Act
- (4) Invasion of Privacy
- (5) Negligence
- (6) Unlawful, Fraudulent and Unfair Business Practices

**Jury Trial Demanded on All Causes of  
Action So Triable**

Electronically Received 10/06/2022 10:41 AM

1 Plaintiff John Doe (“Plaintiff”)<sup>1</sup> brings this action on behalf of himself and all others similarly  
2 situated and for the benefit of the general public against Defendant California Department of Public  
3 Health and Sandra Shewry, Acting Director of the California Department of Public Health, in her official  
4 capacity (collectively referred to as “CDPH” or the “State Defendants”);<sup>2</sup> Thrive Tribe Foundation  
5 (“Thrive Tribe”); Evolve Healthcare, Inc. (“Evolve Healthcare”); Gary Goldstein (“Mr. Goldstein”);  
6 Good Health, Inc. d/b/a Premier Pharmacy Services (“Premier Pharmacy”)<sup>3</sup> (collectively referred to as  
7 the “Non-State Defendants”); and DOES 2–25 (along with State Defendants and Non-State Defendants,  
8 referred to herein as “Defendants”). Plaintiff, through his undersigned counsel, alleges the following  
9 based on personal knowledge as to allegations regarding Plaintiff, and on information and belief as to all  
10 other allegations.

### 11 **NATURE OF THE CLAIM**

12 1. In California, the protection of personal privacy is of paramount importance. The  
13 California Constitution guarantees consumers the right to privacy. Furthermore, California law explicitly  
14 recognizes that for those living with HIV or AIDS, the injury caused by a violation of their personal  
15 medical privacy is particularly harmful.

16 2. This action arises from the conduct of Defendants CDPH, Thrive Tribe, Premier  
17 Pharmacy, Evolve Healthcare, and Mr. Goldstein. These individuals and entities both orchestrated and  
18 participated in, or failed to prevent in the case of CDPH, the unauthorized access of confidential data  
19 from Thrive Tribe belonging to Plaintiff and approximately 460 other individuals enrolled in two CDPH  
20 programs that provide people living with HIV access to adequate healthcare—the AIDS Drug Assistance  
21 Program (“ADAP”) and the Office of AIDS’s Health Insurance Premium Payment program (“OA-  
22 HIPP”). Premier Pharmacy directed its agents Mr. Goldstein and Evolve Healthcare to acquire the Thrive  
23 Tribe data in order to increase its profit in various ways. Thrive Tribe is a contractor for CDPH for  
24

25 \_\_\_\_\_  
26 <sup>1</sup> Due to the sensitive nature of this action, Plaintiff has chosen to file under a pseudonym. (*See, e.g., Jane*  
27 *Doe 8015 v. Sup. Ct.* (2007) 148 Cal.App.4th 489 [patient allowed to proceed anonymously when suing  
28 a laboratory after contracting HIV].)

<sup>2</sup> Following the filing of the initial Complaint, Acting Director Shewry has been succeeded by CDPH’s  
current Director, Dr. Tomás J. Aragón.

<sup>3</sup> Premier Pharmacy was previously identified in the initial Complaint as defendant DOE 1.

1 purposes of enrolling individuals in the ADAP and OA-HIPP programs and administering those  
2 programs.

3 3. When Plaintiff and all other persons similarly situated provided their personal medical  
4 information to CDPH and Thrive Tribe for the purpose of participating in these HIV-assistance programs,  
5 they did so with the reasonable understanding and assurance, either express or implied, that their most  
6 sensitive medical and personal information would be kept confidential and secure.

7 4. Unfortunately for Plaintiff and other similarly situated individuals who participated in  
8 these two programs, which were administered by CDPH with the assistance of Thrive Tribe, their  
9 personal and sensitive medical information was not kept secure. As a result, their confidential information  
10 was disclosed and disseminated without written authorization or consent to at least Mr. Goldstein, Evolve  
11 Healthcare, and Premier Pharmacy and their agents and/or employees.<sup>4</sup>

12 5. According to CDPH's initial investigation of this unauthorized disclosure of confidential  
13 medical information, Joel Anderson, an employee of Thrive Tribe and Evolve Healthcare and an officer,  
14 agent, and/or employee of Premier Pharmacy, disclosed without written authorization or consent from  
15 the affected consumers or CDPH the personal and medical information of Plaintiff and other similarly  
16 situated individuals to at least Mr. Goldstein, Evolve Healthcare, and Premier Pharmacy.

17 6. Neither Mr. Anderson, Evolve Healthcare, Mr. Goldstein, nor Premier Pharmacy were  
18 authorized to access, use, disclose, or permit its employees or agents to use or disclose this information.

19 7. At all times relevant to the unauthorized disclosure of Plaintiff's and other similarly  
20 situated individuals' confidential information, Mr. Anderson and Evolve Healthcare—along with Thrive  
21 Tribe—were deeply and financially connected by and through Mr. Goldstein. Premier Pharmacy also had  
22 a close working and financial relationship with Mr. Goldstein.

23 8. The conduct of Defendants permitted the unauthorized disclosure of sensitive personal  
24 and medical information of HIV-positive individuals and has caused the disclosure of Plaintiff's and  
25

---

26 <sup>4</sup> Adherence Project, which was named in the initial Complaint as a defendant, is a non-profit entity that  
27 has confirmed under penalty of perjury that it is not in possession of any of the data in question and does  
28 not have any assets or insurance. A Request for Dismissal of this entity was filed on September 16, 2022,  
and an Order Granting Dismissal of Adherence Project was issued by the Court on September 19, 2022.  
Adherence Project is not listed as a Defendant in the Amended Complaint for that reason.

1 other similarly situated individuals' HIV status to any person coming in contact with the non-public  
2 personal and sensitive medical information at issue here that was disclosed without their authorization or  
3 consent.

4 9. The non-public personal and medical information at issue here includes, but is potentially  
5 not limited to, their full names, dates of birth, personal phone numbers and email addresses, HIV status  
6 and other medical conditions, health insurance provider information, public health program participant  
7 information, and program eligibility dates.

8 10. Due to the stigma and discrimination associated with HIV, the disclosure of an  
9 individual's HIV status can have far-ranging consequences including loss of housing and employment,  
10 as well as severe health consequences, as a result of the inability to access healthcare services and  
11 increased stress that undermines the immune system.

12 11. Plaintiff and all other similarly situated enrollees also face a long-term battle against  
13 identity theft, as their names, dates of birth, and addresses were subject to the unauthorized disclosure.  
14 One can become a victim of identity theft simply as a result of the unauthorized disclosure of one's name  
15 and address, as this information could be used as a gateway to discovering other personally identifiable  
16 information of the individual, for example by answering security questions with the individual's financial  
17 institutions, or redirecting the individual's mail to an address of the thief's choice.

18 12. The risk of identity theft is further exacerbated because, as part of the ADAP and OA-  
19 HIPP enrollment process, Plaintiff and all others similarly situated provided CDPH and Thrive Tribe  
20 copies of their driver's licenses and/or passports and their IRS Form 1040s or other proofs of income.

21 13. Defendants' collective failure to adequately protect the non-public personal and medical  
22 information in their possession, and the resulting unauthorized disclosures, has caused and will continue  
23 to cause substantial harm and injuries to Plaintiff and Class members.

24 14. Plaintiff brings this action on behalf of himself and others similarly situated for statutory,  
25 actual, and/or compensatory damages; punitive damages<sup>5</sup> and equitable relief, including costs and  
26 expenses of litigation including attorneys' fees; and injunctive relief that may be appropriate for the  
27 benefit both of such persons and the general public.

28 <sup>5</sup> Plaintiff does not seek punitive damages against the State Defendants.

1 **JURISDICTION AND VENUE**

2 15. This Court has jurisdiction over this matter pursuant to California Code of Civil  
3 Procedure section 410.10 because the acts set forth in this Amended Complaint took place in California,  
4 Plaintiff and Class members are citizens of California, and Defendants conduct a substantial amount of  
5 business and/or are incorporated in California.

6 16. Venue is proper in Los Angeles County pursuant to California Code of Civil Procedure  
7 sections 395 and 395.5 and Civil Code section 1798.49, because the Plaintiff resides in this County, a  
8 substantial part of the events and omissions giving rise to the claims occurred in this County as set forth  
9 herein, at least one of the corporate Defendants has their principal place of business in this County, and/or  
10 at least one of the individual Defendants resides in this County.

11 **PARTIES**

12 17. On personal knowledge, Plaintiff John Doe is a citizen of the State of California and  
13 resides in Los Angeles County, California. He is a person living with HIV and, at all times relevant to  
14 this action, was enrolled in the ADAP and OA-HIPP programs, which are state and federally funded  
15 programs to help manage the cost of his HIV treatment. Prior to enrolling in these programs, and at all  
16 times relevant to this action, Plaintiff was not and is not a client of Premier Pharmacy or Evolve  
17 Healthcare. He never purchased HIV medication or any other medications or items from Premier  
18 Pharmacy. John Doe never authorized Evolve Healthcare, Mr. Anderson, Mr. Goldstein, or Premier  
19 Pharmacy to receive, obtain, or retain his personal and medical information. Plaintiff has been damaged,  
20 injured in fact, and/or has lost money or property as a result of Defendants' misconduct, in that he has  
21 had his personal and medical information disclosed to third parties without his authorization, has lost  
22 control over data in which he has a vested interest, and has not received the statutory damages to which  
23 by law he is entitled.

24 18. On October 29, 2020, Plaintiff filed a claim with the State of California under the  
25 California Tort Claims Act. The California Department of General Services has failed to resolve the claim  
26 within the required time period. Plaintiff has thus satisfied any requirement to file a claim prior to  
27 asserting claims in this Amended Complaint against the State Defendants.  
28

1           19. Defendant CDPH is the state agency responsible for implementing the ADAP and OA-  
2 HIPP Programs. It retained Thrive Tribe to act as a contractor and agent to enroll individuals in the ADAP  
3 and OA-HIPP programs as well as to assist in the administration of those programs, and thus was  
4 responsible for overseeing the conduct of Thrive Tribe in the protection of Plaintiff's and other  
5 consumers' personal and medical data and HIV status.

6           20. Defendant Sandra Shewry is the Acting Director of CDPH and is sued herein in her  
7 official capacity.

8           21. Defendant Thrive Tribe Foundation is a 501(c)(3) nonprofit organization with its  
9 principal place of business in the City of West Hollywood, Los Angeles County, California. At all  
10 relevant times herein, Thrive Tribe was a service provider under contract with CDPH focused on, among  
11 other things, enrolling individuals in the ADAP and OA-HIPP programs and assisting CDPH in the  
12 administration of those programs, and acted as an agent of CDPH in that capacity. To enroll clients and  
13 assist CDPH in the administration of these programs, Thrive Tribe was responsible for creating and  
14 maintaining agency records that contained clients' personal and medical information. The conduct of  
15 Thrive Tribe at issue was reviewed, approved, or ratified by one or more of the officers or directors of  
16 Thrive Tribe and/or they had a duty of care and oversight of the conduct that they failed to provide.

17           22. Defendant Evolve Healthcare is a California for-profit corporation with its principal  
18 place of business in Los Angeles County, California. Evolve Healthcare is an agent of or otherwise  
19 affiliated with Defendant Good Health, Inc. d/b/a Premier Pharmacy Services. Mr. Goldstein owns and  
20 operates Evolve Healthcare as his own personal business. The conduct of Evolve Healthcare at issue was  
21 reviewed, approved, or ratified by one or more of the officers or directors of Evolve Healthcare,  
22 specifically including Mr. Goldstein, and/or they had a duty of care and oversight of the conduct that they  
23 failed to provide.

24           23. Defendant Gary Goldstein, also known as "Julian" Goldstein, is the chief executive  
25 officer of Evolve Healthcare. Goldstein is also an employee, agent, or otherwise affiliated with Premier  
26 Pharmacy. Goldstein is also a founder and funder of, and/or otherwise affiliated with, Thrive Tribe and  
27 Adherence Project. Goldstein is a resident of Los Angeles County, California.

1           24. Defendant Good Health, Inc. d/b/a Premier Pharmacy Services is a California for-profit  
2 corporation with its principal place of business in Los Angeles County, California. Premier Pharmacy  
3 was previously identified in the initial Complaint as defendant DOE 1. Defendants Mr. Anderson,  
4 Mr. Goldstein, and Evolve Healthcare are either employees or agents of, or otherwise affiliated with,  
5 Premier Pharmacy, and received compensation from Premier Pharmacy in connection with enrolling  
6 clients with Premier Pharmacy and carrying out other profit-making strategies as described herein. The  
7 conduct of Premier Pharmacy at issue was reviewed, approved, or ratified by one or more of the officers  
8 or directors of Premier Pharmacy and/or they had a duty of care and oversight of the conduct that they  
9 failed to provide. The conduct of Evolve Healthcare, Mr. Goldstein, and Mr. Anderson at issue herein at  
10 issue was also reviewed, approved, and/or ratified by one or more of the officers or directors of Premier  
11 Pharmacy, and/or those officers or directors had a duty of care and oversight of the conduct that they  
12 failed to provide.

13           25. The true names, roles, and capacities of Defendants named as DOES 2 through 25,  
14 inclusive, including their involvement in the wrongdoing at issue, whether individual, corporate,  
15 associate, or otherwise, such as reviewing, approving, or ratifying the conduct at issue, are currently  
16 unknown to Plaintiff and, therefore, are named as Defendants under fictitious names pursuant to  
17 California Code of Civil Procedure section 474. Plaintiff will identify their true identities and their  
18 involvement in the wrongdoing at issue if and when they become known.

19           26. The conduct of certain Defendants described herein was undertaken as agents, servants,  
20 contractors, or employees of CDPH pursuant to California Civil Code section 1798.19 and/or was  
21 performed within the course and scope of their authority, agency, or employment. Thrive Tribe was an  
22 agent of and under contract with CDPH for purposes of the claims at issue, thus making the conduct of  
23 Thrive Tribe's agents and employees, including Mr. Anderson, the responsibility of CDPH.

24           27. CDPH's and Thrive Tribe's conduct described herein was also generally undertaken or  
25 authorized by officers or managing agents who were responsible for supervision and operations decisions  
26 relating to the protection and disclosure of the data in question. CDPH's and Thrive Tribe's actions and  
27 conduct were ratified, authorized, and approved by such managing agents. The described conduct of said  
28 managing agents and individuals was therefore undertaken on behalf of CDPH and Thrive Tribe. CDPH

1 and Thrive Tribe further had or are imputed to have advance knowledge of the actions and conduct of  
2 said individuals.

3 28. The Non-State Defendants were agents or employees of each other, as set forth herein.  
4 Said Defendants are jointly and severally responsible, in whole or in part, for the conduct, damages, and  
5 injuries alleged herein. At all relevant times, the Non-State Defendants engaged in a calculated and  
6 coordinated campaign of silence because the prospect of significant future profits outweighed concerns  
7 regarding the privacy and sensitivity of such data, all to the significant detriment of the public and  
8 Plaintiff and Class members.

9 29. In addition, the Non-State Defendants had a vested financial interest in not disclosing the  
10 scope and extent of the unauthorized disclosure of information, thereby aiding and abetting the violations  
11 of law set forth herein, since without their active involvement and participation, these unauthorized  
12 disclosures would not have taken place. The Non-State Defendants are active participants in the  
13 conspiracy or concerted action at issue herein.

14 30. Each of the above-named Non-State Defendants acted in concert and both aided and  
15 abetted and conspired with each other not to disclose the material facts stated herein. This conduct was  
16 authorized or acted on by and through their respective officers, employees, agents, servants, and/or  
17 representatives. The Non-State Defendants engaged in a conspiracy, or otherwise acted in concert, to  
18 (i) disclose and profit from the personal and confidential medical information at issue herein, and  
19 (ii) withhold material information about the unauthorized disclosure from the public, Plaintiff, and Class  
20 members. It was due to this conspiracy, aiding and abetting, or concerted action that Plaintiff and each  
21 Class member suffered harm.

### 22 **FACTUAL ALLEGATIONS**

23 31. A national survey conducted in 2012 by *The Washington Post*/Kaiser Family Foundation  
24 Survey Project found that fewer than half of respondents indicated that they would feel “very  
25 comfortable” working with someone who has HIV or AIDS. (*The Washington Post* and Kaiser Family  
26 Foundation, *2012 Survey of Americans on HIV/AIDS Summary and Chartpack* (July 2012) at 16,  
27 <https://www.kff.org/wp-content/uploads/2013/01/8334-f.pdf>.) Only a third of respondents indicated that  
28



1 they would feel “very comfortable” having a roommate who is HIV-positive, and fewer than a quarter  
2 would feel “very comfortable” having food prepared by someone who is HIV-positive. (*Ibid.*)

3 32. A 2016 meta-analysis published in the journal *AIDS and Behavior* concluded anxiety  
4 related to the disclosure of one’s HIV status is “highly prevalent.” (Michael Evangeli and Abigail L.  
5 Wroe, *HIV Disclosure Anxiety: A Systematic Review and Theoretical Synthesis*, *AIDS Behavior* (2017)  
6 at 21:4, [https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5216111/pdf/10461\\_2016\\_Article\\_1453.pdf](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5216111/pdf/10461_2016_Article_1453.pdf).)  
7 The meta-analysis reviewed 119 studies, which the authors concluded “demonstrated that perceived  
8 interpersonal risks are associated with HIV disclosure and outlined evidence of associations with anxiety,  
9 fear and worry.” (*Id.* at 1.)

10 33. Recent studies further demonstrate that even if people living with HIV, or at risk of  
11 contracting HIV, do not know and cannot demonstrate who may have been made aware of their health  
12 status, acts such as the conduct alleged herein increase stress and anxiety due to the very real risks of the  
13 loss of housing, relationships, and employment. (*See* Activities Combating HIV Stigma and  
14 Discrimination, HIV.gov, [https://www.hiv.gov/federal-response/federal-activities-agencies/activities-](https://www.hiv.gov/federal-response/federal-activities-agencies/activities-combating-hiv-stigma-and-discrimination)  
15 [combating-hiv-stigma-and-discrimination](https://www.hiv.gov/federal-response/federal-activities-agencies/activities-combating-hiv-stigma-and-discrimination) (last visited Oct. 5, 2022).) “HIV stigma and discrimination  
16 can pose complex barriers to prevention, testing, treatment, and support for people living with or at risk  
17 for HIV. Some examples of stigma include being shunned by family, peers, and the wider community;  
18 receiving poor treatment in health care and education settings; and experiencing judgmental attitudes,  
19 insults, or harassment. Some individuals with HIV have been denied or lost employment, housing, and  
20 other services; prevented from receiving health care; denied access to educational and training programs;  
21 and have been victims of violence and hate crimes. HIV-related stigma and discrimination prevents  
22 individuals from learning their HIV status, disclosing their status even to family members and sexual  
23 partners, and/or accessing medical care and treatment, weakening their ability to protect themselves from  
24 getting or transmitting HIV, and to stay healthy.” (*Ibid.*)

25 34. As a result, even in 2022, despite key advancements in the prevention and treatment of  
26 HIV and AIDS, disclosure of one’s HIV status is still widely perceived as socially dangerous. For people  
27 living with HIV or at risk of HIV, their personal health medical information is considered to be  
28

1 sacrosanct. Therefore, any person who lives with HIV or is at risk of contracting HIV should have full  
2 control over when and with whom this information is shared.

3 **CDPH's Healthcare Programs for Individuals with HIV and AIDS**

4 35. CDPH's Office of AIDS has lead responsibility for coordinating state programs, services,  
5 and activities relating to HIV and AIDS. CDPH's Office of AIDS administers ADAP, through which  
6 CDPH pays the prescription costs for many medications commonly prescribed individuals living with  
7 HIV and those at risk of contracting HIV. CDPH also administers the OA-HIPP program, which  
8 subsidizes health insurance premiums and certain outpatient medical out-of-pocket costs for eligible  
9 HIV-positive Californians who are co-enrolled in ADAP.

10 36. In the course and scope of administering these programs, CDPH contracts with for-profit  
11 and nonprofit entities to help administer the ADAP and OA-HIPP programs for approximately 30,000  
12 Californians.

13 37. Thrive Tribe was a CDPH contactor and service provider for people living with HIV and  
14 AIDS during all times relevant to this action. In that capacity, Thrive Tribe and its employees and/or  
15 agents, including Mr. Anderson and Mr. Goldstein, were provided with and had access to highly  
16 confidential and sensitive personal and medical information of enrollees in these CDPH programs,  
17 including that of Plaintiff. Attached as Exhibit 1 and incorporated by this reference is the contract between  
18 CDPH and Thrive Tribe, which outlines CDPH's various responsibilities to train Thrive Tribe personnel  
19 and oversee Thrive Tribe and Thrive Tribe and its employees' and agents' obligations to protect and  
20 secure such data.

21 38. In approximately April 2018, Plaintiff enrolled in ADAP and OA-HIPP through Thrive  
22 Tribe.

23 39. To enroll in ADAP and OA-HIPP, Plaintiff provided his HIV status, medical history, and  
24 other non-public personal and financial information to Thrive Tribe and CDPH.

25 40. This medical, personal, and financial information is required by CDPH in order for  
26 individuals to receive the CDPH subsidy that pays the monthly prescription drug costs and/or health  
27 insurance premiums for ADAP and OA-HIPP clients.

1           41. In its capacity as a CDPH contractor and agent, Thrive Tribe created and maintained  
2 records regarding Plaintiff and other similarly situated individuals that it enrolled in ADAP and OA-  
3 HIPP. This included records such as enrollees' full names, dates of birth, personal phone numbers and  
4 email addresses, HIV status and other medical conditions, financial information for determining  
5 eligibility, health insurance provider information, public health program participant information, and  
6 program eligibility dates.

7           42. These records were created and maintained at the direction of CDPH by Thrive Tribe in  
8 furtherance of the operation of CDPH's ADAP and OA-HIPP programs.

9           43. As custodians of private health information, CDPH and Thrive Tribe are required by state  
10 law to ensure that such information is not disclosed or disseminated to any unauthorized parties without  
11 the clients' advance written authorization or consent.

12           **The Unauthorized Disclosure of Highly Confidential Information by Thrive Tribe**

13           44. On or about April 30, 2020, CDPH was notified that the personal and medical  
14 information of approximately 460 individuals enrolled in ADAP and OA-HIPP had been the subject of  
15 an unauthorized disclosure by Mr. Anderson, an employee of Thrive Tribe and Evolve Healthcare and  
16 an officer, agent, and/or employee of Premier Pharmacy. As described below, CDPH's subsequent  
17 notification to the affected individuals was incomplete.

18           45. Even though, as detailed herein, the disclosure in question took place in April 2019, none  
19 of the Non-State Defendants told CDPH of the unauthorized disclosure at that time or otherwise  
20 participated in the subsequent notification of the affected individuals, despite their duty to do so.

21           46. In subsequent communications with Plaintiff and his counsel, CDPH revealed that Thrive  
22 Tribe was the contractor responsible for the unauthorized disclosure. According to CDPH, Mr. Anderson  
23 obtained the personal and medical information at the direction of Mr. Goldstein and Premier Pharmacy  
24 and disclosed it to Mr. Goldstein and Premier Pharmacy, though neither were authorized to receive it.

25           47. On or around June 30, 2020—two months after the CDPH was notified of the  
26 unauthorized disclosure—CDPH alerted Plaintiff and approximately 460 other similarly situated  
27 individuals by regular mail that their non-public personal and medical information was the subject of an  
28

1 unauthorized disclosure and had been compromised (“CDPH Mailing”). Attached as Exhibit 2 and  
2 incorporated herein by reference is a true and correct copy of the CDPH Mailing.

3 48. This communication has not been published on either CDPH’s website or the California  
4 or federal data breach notification databases as of the time the original Complaint and this Amended  
5 Complaint were filed. Nor have any of the Non-State Defendants apparently notified the relevant  
6 authorities of their role in this breach, including but not limited to the U.S. Department of Health and  
7 Human Services and the California Department of Justice. In addition, while CDPH claims in the Thrive  
8 Tribe Breach FAQ discussed below that it is “attempting to retrieve” Plaintiff’s and other similarly  
9 situated individuals’ data, CDPH has failed to do so.

10 49. Thus, as of this Amended Complaint, it appears the data in question has not been  
11 remediated in terms of: (1) identifying all locations of that data and who has had contact with it;  
12 (2) securing the data against further unauthorized disclosures; and (3) informing Plaintiff and Class  
13 members the full details of the unauthorized disclosures, who has had access to the data, and what has  
14 and will be done to prevent further unauthorized disclosures.

15 50. As evidence of the ineffectual training CDPH provides its ADAP and OA-HIPP  
16 contractors and agents, including Thrive Tribe, and the inadequate security controls the agency uses for  
17 its ADAP and OA-HIPP programs, CDPH’s investigation revealed that the unauthorized disclosure  
18 occurred almost a full year before CDPH was alerted of the data breach—“on around April 22, 2019.”

19 51. According to the CDPH Mailing to Plaintiff and others similarly situated, this  
20 unauthorized disclosure may have included the full names, dates of birth, personal phone numbers and  
21 email addresses, health insurance provider information, public health program participant information,  
22 and program eligibility dates of individuals enrolled in ADAP and/or OA-HIPP that were accessible to  
23 Thrive Tribe in its capacity as a CDPH contractor and agent.

24 52. Although the CDPH communication claims that the unauthorized disclosure did not  
25 include Social Security numbers or driver’s license numbers, Plaintiff and others similarly situated  
26 provided that type of information to Thrive Tribe and CDPH for the purpose of enrolling and maintaining  
27 eligibility in the ADAP and OA-HIPP Programs.

1           53. Plaintiff and others similarly situated did not discover and reasonably could not have  
2 discovered until receipt of CDPH’s June 30, 2020 letter (the CDPH Mailing) that their personal and  
3 medical information was the subject of an unauthorized disclosure.

4           54. The Non-State Defendants have neglected to provide details concerning how Plaintiff’s  
5 and Class members’ personal and medical information was obtained and shared by Mr. Anderson, or any  
6 other information that would aid in the efforts of these individuals to protect against further unauthorized  
7 disclosures of their HIV-positive status or the risk of identity theft or fraud.

8           55. Nor has the CDPH sent any further explanation to Class members in a direct  
9 communication relaying further facts underlying this unauthorized disclosure; for example, what  
10 personal and medical information has been disclosed and by whom, where the data may reside, and how  
11 Class members may ensure that data is deleted.

12           56. In the CDPH Mailing notifying Plaintiff and others similarly situated of this unauthorized  
13 disclosure, CDPH did not even identify the CDPH contractor responsible for the unauthorized disclosure  
14 of their personal and medical information.

15           57. Because the protection of his personal and medical information is of the utmost  
16 importance to Plaintiff, knowing that this information is “floating out there,” accessible to unknown  
17 thieves and unauthorized entities, is “gut wrenching,” according to Plaintiff. It is especially traumatizing  
18 to have this information exposed by the healthcare professionals he trusted the most to protect it. He has  
19 since experienced fear, anxiety, and worry caused by the unauthorized disclosure of his medical  
20 information based on the notice from CDPH.

21           58. In an attempt to address the fear, anxiety, and worry caused by the unauthorized  
22 disclosure of his medical information and mitigate the risk of becoming a victim of identity theft, Plaintiff  
23 submitted on or about July 23, 2020 a “grievance” form to ADAP, seeking to identify which CDPH  
24 contractor was involved in the unauthorized disclosure referenced in the CDPH Mailing, what  
25 information had been disclosed, and to whom this personal and medical information was disclosed  
26 without authorization.

27           59. On or about July 31, 2020, CDPH responded to Plaintiff’s grievance by phone call.  
28 CDPH informed Plaintiff that Thrive Tribe was the agent and contractor responsible for the unauthorized

1 disclosure of Plaintiff's and other similarly situated individuals' personal and medical information.  
2 According to CDPH, these individuals' HIV status was among the information included in this  
3 unauthorized disclosure.

4         60. In or about July 2020, Plaintiff's counsel submitted two Public Records Act ("PRA")  
5 requests to CDPH seeking more information about the unauthorized access. Attached as Exhibit 3 and  
6 incorporated herein by this reference is a true and correct copy of one of the documents CDPH provided  
7 Plaintiff's counsel in response to the PRA Requests entitled "Frequently Asked Questions," which  
8 summarizes the results of CDPH's investigation (hereinafter, the "Thrive Tribe Breach FAQ" or "FAQ").  
9 According to a cover letter to Plaintiff's counsel from CDPH accompanying the Thrive Tribe Breach  
10 FAQ, the personal and medical information of Plaintiff and approximately 460 similarly situated  
11 individuals was disclosed without authorization "to three unauthorized health-related entities, including  
12 a pharmacy benefits company, an entity trying to become an ADAP enrollment site, and a health care  
13 coordination company." (*Id.* at 2.) The FAQ has not been posted on the CDPH website, and instead  
14 appears to only have been made available to Class members in response to individual inquiries. CDPH  
15 has not advised Class members how to access this information or even that it is available to Class  
16 members.

17         61. According to the Thrive Tribe Breach FAQ, the personal and medical information of  
18 these approximately 460 individuals was disclosed by Thrive Tribe without authorization or advance  
19 consent to Mr. Goldstein, Evolve Healthcare, and Premier Pharmacy. (*Ibid.*)

20         62. According to CDPH's Thrive Tribe Breach FAQ and other documents provided by  
21 CDPH in response to the PRA requests, on or about April 22, 2019, Mr. Anderson accessed sensitive  
22 information of approximately 460 individuals enrolled in ADAP and/or OA-HIPP that was maintained  
23 by Thrive Tribe. Mr. Anderson thereafter, and without authorization from Plaintiff or Class members,  
24 uploaded the Thrive Tribe data to a third-party cloud-based server, detailed below. He provided access  
25 to some of that information to Evolve Healthcare, Mr. Goldstein, and Premier Pharmacy, who in turn  
26 copied that information to computers in their possession, custody, or control. Plaintiff's and others'  
27 personal and medical information, including their HIV status, was included in this improperly accessed  
28 data, according to CDPH.

1           63. As a direct and foreseeable result of CDPH's failure to oversee the actions of its  
2 contractor and agent Thrive Tribe and its employees and staff, Mr. Anderson was able to engage in this  
3 unauthorized disclosure undetected for over a year.

4           64. CDPH produced additional documents to Plaintiff's counsel in response to Plaintiff's  
5 PRA requests that corroborate the findings of Plaintiff's investigation and the allegations contained  
6 herein.

7           65. Based on these communications and documents obtained from CDPH and Plaintiff's  
8 counsel's own investigation, Plaintiff's counsel sent letters in August 2020 to Thrive Tribe, Adherence  
9 Project, Evolve Healthcare, Premier Pharmacy, and numerous individuals serving as officers or board  
10 members of those organizations, including Mr. Anderson and Mr. Goldstein, demanding that they cure  
11 and correct this illegal conduct as described herein. While one of Thrive Tribe's directors responded to  
12 the August 3 letter, he did not provide any specifics that rebutted the information provided in Plaintiff's  
13 letter and by CDPH, nor did he offer to cure the unauthorized disclosure. Instead, the director did not  
14 deny such disclosure took place, but asserted (without providing any corroborating information) that  
15 CDPH's notification of the unauthorized disclosure was "in error" and that the agency failed to  
16 adequately investigate and fully adjudicate the matter. The information so far provided by CDPH refutes  
17 such claims.

18           66. As of the date of this Amended Complaint, each of the Non-State Defendants are still in  
19 possession of the data at issue and have not taken appropriate remedial steps to identify, segregate, and/or  
20 protect such data against further unauthorized disclosure. In addition, even though it was data under  
21 Thrive Tribe's control, Thrive Tribe never disclosed the facts surrounding this unauthorized disclosure  
22 on its website or to its members.

23                   **Mr. Goldstein, Evolve Healthcare, and Premier Pharmacy's Involvement in the**  
24                   **Unauthorized Disclosure**

25           67. Information obtained during the course of Plaintiff's investigation into the unauthorized  
26 disclosure at issue demonstrates that Mr. Goldstein orchestrated and is jointly responsible for the  
27 unauthorized disclosure, which resulted in financial gain to Evolve Healthcare and Premier Pharmacy.  
28

1 Mr. Goldstein provides a clear and direct link between the unauthorized disclosure of the personal and  
2 medical information at issue and the unauthorized recipients of this data identified by CDPH.

3 68. Mr. Goldstein was one of the initial founders and a former CEO of Thrive Tribe. He also  
4 provided the initial funding to start the organization and continues to financially support the organization.

5 69. Although he claims to have officially left the organization in or about October 2014,  
6 Mr. Goldstein continued to remain actively involved in Thrive Tribe.

7 70. As early as 2014, Mr. Goldstein was known “for pressuring Thrive Tribe members to  
8 shift their drug prescriptions to pharmacies with which he was connected.” (*See Fight Between*  
9 *Two WeHo HIV Groups Opens a Dirty Window*, WEHoville (Oct. 17, 2016),  
10 <https://www.wehoville.com/2016/10/17/fight-two-hiv-groups-opens-dirty-window/>.)

11 71. In October 2016, Thrive Tribe was sued by Kevin Stalter, its CEO at the time.

12 72. Due to the economic uncertainty of the lawsuit, which threatened the continued viability  
13 of Thrive Tribe, Mr. Goldstein came up with the idea to set up Adherence Project “to be the successor  
14 organization to Thrive Tribe Foundation’s (TTF) Connection to Care (Site 1966)” and to take over work  
15 on behalf of CDPH in the OA-HIPP and ADAP programs, according to documents provided by CDPH  
16 to Plaintiff’s counsel.

17 73. As a result, in addition to his role as the chief executive officer of Evolve Healthcare,  
18 Mr. Goldstein also became the initial founder of Adherence Project and continued to have a financial  
19 interest in the organization, as well as apparently having a continued interest in and control over Thrive  
20 Tribe.

21 74. According to documents produced in response to Plaintiff’s PRA requests, at the behest  
22 of Mr. Goldstein, who was operating at the direction of Premier Pharmacy, in April 2019 Mr. Anderson  
23 accessed what has been referred to as “The Thrive Tribe Client Log” from Thrive Tribe’s database, which  
24 contained Plaintiff’s and other similarly situated individuals’ personal and medical information.  
25 Mr. Anderson subsequently “electronically sent to Gary ‘Julian’ Goldstein” and Evolve Healthcare staff  
26 this data, even though at the time Mr. Goldstein was no longer an employee or agent of Thrive Tribe,  
27 without Plaintiff’s or the putative Class’s written consent and/or authorization. Mr. Goldstein “sent Joel  
28 Anderson . . . to obtain[]” the Thrive Tribe Client Log “for him,” according to CDPH documents. The



1 data was then used to financially benefit Premier Pharmacy as discussed below, and a significant portion  
2 of the data was uploaded to Premier Pharmacy’s patient prescription drug database.

3 75. Neither Mr. Goldstein, his company Evolve Healthcare, nor Premier Pharmacy was a  
4 CDPH-certified enrollment/eligibility worker at any time relevant herein, which means, *inter alia*, they  
5 were not authorized by CDPH to receive or use the Thrive Tribe Client Log or any data contained therein.  
6 Nor were Mr. Goldstein or Evolve Healthcare authorized by Plaintiff or others similarly situated to  
7 receive, use, or cause to be disclosed their personal and medical information. Mr. Goldstein and his  
8 company Evolve Healthcare and Premier Pharmacy were therefore unauthorized recipients of this  
9 confidential information.

10 76. Mr. Anderson obtained the Thrive Tribe Client Log under the pretense that he was a  
11 CDPH-certified enrollment/eligibility worker volunteering at Thrive Tribe, where he assisted people  
12 enrolling in the ADAP and OA-HIPP programs.

13 77. However, concurrently and at all times relevant herein, Mr. Anderson was also an  
14 employee or agent of, or otherwise affiliated with, Evolve Healthcare and Premier Pharmacy, and thus  
15 according to documents obtained from CDPH was “working for Evolve Healthcare/Julian  
16 Goldstein/Adherence Project.”

17 78. According to CDPH’s investigation, there was a financial motivation for Evolve  
18 Healthcare, Premier Pharmacy, Mr. Anderson, and Mr. Goldstein to engage in the unauthorized sharing  
19 of the data at issue. Mr. Goldstein “wanted the [Thrive Tribe] client list to increase traffic to his new  
20 enrollment site [*i.e.*, Adherence Project] and he would receive payment for clients that he brought to  
21 Premier Pharmacy.”

22 79. Evolve Healthcare and Mr. Goldstein had an agreement with Premier Pharmacy that, in  
23 exchange for referring enrollees in the ADAP and OA-HIPP programs to Premier Pharmacy for the  
24 purchase of their HIV medications, Premier Pharmacy provided financial compensation.

25 80. According to the documents obtained from the CDPH, Plaintiff’s and other similarly  
26 situated individuals’ personal and medical information that Mr. Anderson provided to Mr. Goldstein  
27 “was input into a database” used by Mr. Goldstein, Mr. Anderson, and Evolve Healthcare “to track  
28 HIV/PrEP clients,” for the mutual financial benefit of Evolve Healthcare and Premier Pharmacy. “PrEP”

1 means “Pre-Exposure Prophylaxis” and includes the use of anti-HIV medications to keep HIV-negative  
2 people from becoming infected.

3 81. Mr. Goldstein directed Mr. Anderson to identify a database platform where various lists  
4 maintained by Evolve Healthcare could be stored. Mr. Anderson thereafter set up a database in a third-  
5 party cloud-based server serviced by Airtable. The personal and medical information at issue was  
6 uploaded to that database platform by Mr. Anderson, again without the authorization or consent of  
7 Plaintiff and others similarly situated.

8 82. This was not a trivial project, as Mr. Anderson claimed he spent over 50 hours creating  
9 this database and uploading the database into this cloud-based server.

10 83. In 2019, Evolve Healthcare was managing several lists in its possession, including lists  
11 of clients referred to Premier Pharmacy by Evolve Healthcare, Mr. Anderson, and Mr. Goldstein, as well  
12 as lists of individuals who were not Premier Pharmacy clients who could be targeted for referral.

13 84. These lists were created from the Thrive Tribe Client Log, among other sources, and  
14 were created for the financial benefit of Mr. Goldstein, Evolve Healthcare, and Premier Pharmacy. At  
15 the time these lists were being developed, Premier’s CEO provided Evolve Healthcare, Mr. Goldstein,  
16 and Mr. Anderson lists of Premier Pharmacy patients.

17 85. Evolve Healthcare’s employees worked in close coordination with and at the direction of  
18 Premier Pharmacy staff, including its CEO.

19 86. According to CDPH’s investigatory documents, some or all of the data derived from the  
20 “[Thrive Tribe Client Log] was saved to Premier Pharmacy’s database” by Mr. Anderson and/or  
21 Mr. Goldstein.

22 87. This data was also uploaded by Evolve Healthcare employees to Premier Pharmacy’s  
23 patient prescription drug database. Premier Pharmacy was an unauthorized recipient of this confidential  
24 information.

25 88. On or about July 7, 2020, CDPH served Evolve Healthcare with a “Clawback Letter,”  
26 notifying Evolve Healthcare that the agency was informed that “The Thrive Tribe Client Log: a list of  
27 active clients of The Thrive Tribe as of April 2019,” which included Plaintiff’s and others’ personal and  
28

1 medical information, “was provided” to Evolve Healthcare “without authorization.” Attached as  
2 Exhibit 4 and incorporated herein by reference is a true and correct copy of that document.

3 89. Evolve Healthcare and Mr. Goldstein have tried to avoid culpability for this unauthorized  
4 disclosure, claiming that “Evolve Healthcare did not receive, on or around April 22, 2019, electronic  
5 information titled ‘Thrive Tribe Client Log,’ or a list of active clients of Thrive Tribe as of April 2019,  
6 and does not now have any such information.” While there may not be a list technically called “Thrive  
7 Tribe Client Log” on a computer under the possession or control of Evolve Healthcare and/or  
8 Mr. Goldstein, Mr. Goldstein was directly provided the data in question by Mr. Anderson, and  
9 Mr. Anderson set up a database containing the data. Mr. Goldstein, in his capacity as the CEO of Evolve  
10 Healthcare, had access to the database and was also able to download the data from the third-party cloud-  
11 based server Airtable.

12 **Evolve Healthcare Worked in Concert with Premier Pharmacy**

13 90. During all times relevant to this Amended Complaint, Evolve Healthcare worked nearly  
14 exclusively with Premier Pharmacy. Evolve Healthcare’s, and by extension Mr. Goldstein’s, income is  
15 derived in part from this relationship with Premier Pharmacy. Evolve Healthcare operates as a fully  
16 integrated “marketing arm” of Premier Pharmacy, providing client management and profit-boosting  
17 services across Premier’s book of business.

18 91. Mr. Anderson also works with Evolve Healthcare and Premier Pharmacy.

19 92. Evolve Healthcare’s specific role with Premier Pharmacy is to undertake profit-  
20 maximization schemes on behalf of and with the agreement and assent of the pharmacy. For its work  
21 with Premier, Evolve Healthcare had access to Premier’s computer network, including a patient  
22 prescription database and a portal for communicating with patients’ doctors. In furtherance of this  
23 agreement, Mr. Goldstein, Mr. Anderson, and Evolve Healthcare staff were able to access Premier’s  
24 computer network and client databases, using laptops issued to them by Premier Pharmacy and/or remote  
25 network access via their personal computers, and could use those computers to access and/or upload some  
26 or all of the data in question to Premier Pharmacy’s network, even though they did not have prior  
27 authorization or consent from Class members to do so. Evolve Healthcare employees were required to  
28 use Premier’s patient database and closely coordinate with Premier’s staff as an essential aspect of the

1 HIV patient services that Premier Pharmacy hired Evolve Healthcare to provide. This work was  
2 undertaken for the financial benefit of Premier Pharmacy and required Mr. Goldstein, Mr. Anderson, and  
3 Evolve Healthcare staff to use Premier's patient database.

4 93. The profit-generating efforts by Evolve Healthcare, on behalf of and with the assent of  
5 Premier Pharmacy, include, but are not limited to: (1) soliciting Premier Pharmacy's HIV-positive clients,  
6 including persons whose data was obtained from Thrive Tribe without their authorization or consent, to  
7 transfer their medical care to doctors who participate in the federal 340B Drug Pricing Program under  
8 the Medicaid Drug Rebate Program, with the intent that thereafter these individuals would use Premier  
9 Pharmacy to fulfill prescriptions; (2) influencing Premier Pharmacy clients, including persons whose data  
10 was obtained from Thrive Tribe without their authorization or consent, who were prescribed antiretroviral  
11 medications for their HIV diagnoses to switch their medication regimen from a one-pill treatment to a  
12 three-pill treatment, as the multi-pill regimen generates more profits; and (3) soliciting individuals,  
13 including persons whose data was obtained from Thrive Tribe without their authorization or consent,  
14 who are prescribed medications related to the prevention and/or treatment of HIV/AIDS for referral to  
15 the pharmacy.

16 94. Under the 340B Drug Pricing Program, a healthcare organization like Premier Pharmacy  
17 is eligible to purchase covered medications at an estimated 25–50% discount, which can make filling  
18 such prescriptions profitable for Premier Pharmacy, and by extension, benefit Evolve Healthcare,  
19 Mr. Anderson, and Mr. Goldstein.

20 95. Mr. Anderson, Mr. Goldstein, Evolve Healthcare, and Premier Pharmacy were  
21 financially motivated to enter into an agreement to move clients to doctors and clinics that participated  
22 in the 340B Drug Pricing Program in order to boost Premier Pharmacies' profits, which would include  
23 persons whose data was obtained from Thrive Tribe without their authorization or consent.

24 96. Soliciting existing Premier patients to switch from their current doctors and clinics to  
25 340B clinics and doctors (and the profits that this generated for Premier) drove Mr. Goldstein's conduct  
26 related to the data breach.

27 97. Evolve Healthcare and Mr. Goldstein engaged in various other schemes at the direction  
28 of, with the knowledge of, and for the benefit of Premier Pharmacy.

1           98. Premier Pharmacy personnel and Mr. Goldstein directed Mr. Anderson to become an  
2 ADAP enrollment worker at Thrive Tribe so that Evolve Healthcare and Mr. Goldstein could access  
3 Thrive Tribe’s membership for Premier’s profit. Mr. Anderson, who was simultaneously a volunteer of  
4 Thrive Tribe and an agent, employee, or contractor of Premier Pharmacy, Evolve Healthcare, and  
5 Mr. Goldstein, disclosed or caused to be disclosed, without written authorization from CDPH or these  
6 individuals, the Thrive Tribe membership list and their HIV statuses to Premier Pharmacy, Evolve  
7 Healthcare, and Mr. Goldstein.

8           99. Evolve Healthcare, Mr. Goldstein, and Mr. Anderson acted as the agents of Premier  
9 Pharmacy when they obtained without authorization the nonpublic personal and medical information of  
10 the 460 individuals held by Thrive Tribe. Premier Pharmacy exercised a significant level of control over  
11 Evolve Healthcare’s operations in pursuit of a common purpose of increasing Premier’s profits. Premier  
12 relied on Mr. Goldstein’s and Evolve Healthcare’s judgment to develop strategies to increase Premier’s  
13 profits. Premier Pharmacy, after learning of Mr. Goldstein’s various misconducts, including his intent to  
14 obtain the Thrive Tribe membership list in order to increase Premier’s profits, continued Premier’s  
15 ongoing business relationship with Evolve Healthcare and Mr. Goldstein.

16                   **CDPH’s and Thrive Tribe’s Failure to Prevent the Unauthorized Disclosure**

17           100. According to the CDPH Office of AIDS’s Agreement by Employee/Contractor to  
18 Comply With Confidentiality Requirements, CDPH purportedly recognizes that the confidentiality of  
19 personal and medical records of people living with HIV/AIDS must be of the “the foremost concern” to  
20 its contractors and employees. Attached as Exhibit 5 and incorporated herein by reference is a true and  
21 correct copy of that document.

22           101. Public health agencies and service providers such as CDPH, its contractors such as Thrive  
23 Tribe, and its employees and agents are legally required to keep their clients’ personal and medical  
24 information private and secured.

25           102. Yet despite undertaking this responsibility, CDPH, through the actions or inactions of its  
26 agent and contractor, Thrive Tribe and Thrive Tribe’s employees failed to protect the unauthorized  
27 disclosure of Plaintiff’s and other similarly situated individuals’ personal and medical information.  
28

1           103.    CDPH and Thrive Tribe either knew or reasonably should have known of the risks  
2 inherent in maintaining ADAP and OA-HIPP clients' non-public personal and medical information, and  
3 knew or reasonably should have known that if such information was disclosed to persons who were not  
4 authorized to possess it, the disclosure could have dire consequences for Plaintiff and Class members.

5           104.    Thrive Tribe and its directors were aware that Mr. Goldstein formed Thrive Tribe to  
6 create a pipeline of patient referrals for Evolve Healthcare and Premier Pharmacy, monetizing for his and  
7 Premier's financial benefit the organization's work in the West Hollywood community. As Thrive Tribe's  
8 founder and primary initial funder, controlling director, and past executive director, Mr. Goldstein's  
9 schemes were no secret to Thrive Tribe's directors and staff. Thrive Tribe's participation in the  
10 unauthorized access of the data was motivated by its need to continue receiving financial support from  
11 Mr. Goldstein.

12           105.    In fact, the unauthorized disclosure alleged herein is not the first occurrence where a  
13 former Thrive Tribe employee was suspected of disclosing the personal and medical information of  
14 hundreds of HIV-positive individuals who were clients of Thrive Tribe without their authorization or  
15 consent, many of whom would have been ADAP or OA-HIPP enrollees.

16           106.    In or about July 2016, shortly after Thrive Tribe's then-CEO Kevin Stalter was  
17 terminated (which led to Stalter's lawsuit against Thrive Tribe later that year and Mr. Goldstein's plan to  
18 establish Adherence Project in response, as alleged above), the personal and private data of the Thrive  
19 Tribe's members was accessed without authorization. (*See Fight Between Two WeHo HIV Groups Opens*  
20 *a Dirty Window*, WEHOville (Oct. 17, 2016), [https://www.wehoville.com/2016/10/17/fight-two-hiv-](https://www.wehoville.com/2016/10/17/fight-two-hiv-groups-opens-dirty-window/)  
21 [groups-opens-dirty-window/](https://www.wehoville.com/2016/10/17/fight-two-hiv-groups-opens-dirty-window/).)

22           107.    According to that report, Thrive Tribe alleged that Mr. Stalter illegally downloaded the  
23 organization's database for the apparent purpose of creating a competing nonprofit organization. (*Ibid.*)  
24 The database that Mr. Stalter allegedly accessed contained the names of and other information about  
25 Thrive Tribe's members, many of whom are HIV-positive. (*Ibid.*)

26           108.    Although Thrive Tribe asked the L.A. County Sheriff's Department to investigate this  
27 situation and did not report to CDPH that it had been resolved, CDPH continued to work with Thrive  
28

1 Tribe in its capacity as a CDPH contractor. CDPH thus failed to terminate its contract with Thrive Tribe  
2 after receiving notice of this possible privacy breach.

3 109. In addition, despite having knowledge that its former CEO Mr. Stalter may have been  
4 able to improperly access the personal, medical, and financial data of the organization's clients and  
5 members, CDPH and Thrive Tribe failed to take necessary steps to audit or prevent future unauthorized  
6 disclosures of such information, as evidenced by the efforts of Mr. Anderson that went undetected for a  
7 year.

8 110. It was not until June 17, 2020, after CDPH was notified of the most recent unauthorized  
9 disclosure of Thrive Tribe's clients' personal and medical information, that CDPH terminated Thrive  
10 Tribe's ADAP contract. CPDH also declined to authorize Adherence Project to take over the operations  
11 of Thrive Tribe as a successor organization, likely in part because of Mr. Goldstein's role in obtaining  
12 unauthorized access to and disclosure of Plaintiff's and Class members' sensitive personal data.

13 111. CDPH still has not adequately notified all other individuals affected by this unauthorized  
14 disclosure that the unauthorized disclosure of their personal and medical information arose from Thrive  
15 Tribe's failures to adequately protect such information, even though it is obligated by both law and its  
16 contract with CDPH to do so. Nor has CDPH alerted the Class members that Mr. Goldstein,  
17 Mr. Anderson, and Evolve Healthcare—along with Thrive Tribe and Premier Pharmacy—received some  
18 or all of this data and are jointly and severally responsible for this unauthorized disclosure.

19 112. As a result of the unlawful conduct described above, all of the Defendants breached  
20 duties owed to Plaintiff and Class members by, *inter alia*, (i) not exercising reasonable care in retaining,  
21 maintaining, securing, and safeguarding non-public personal and medical information from being  
22 accessed and taken by unauthorized persons, including by present and former employees; (ii) failing to  
23 implement processes to detect a breach or unauthorized access in a timely manner and to act upon any  
24 warnings or alerts that such systems had been improperly accessed; (iii) failing to timely and fully  
25 disclose the facts surrounding this unauthorized access to Plaintiff and Class members; (iv) uploading  
26 and accessing or permitting the uploading and accessing of such data without advance authorization and  
27 consent to do so; and/or (v) failing to disclose that Defendants had not adequately secured Plaintiff's or  
28 Class members' personal and medical information.

1 113. Despite requests to all Defendants to take appropriate action, to date this unauthorized  
2 disclosure remains unremedied.

3 **CLASS ALLEGATIONS**

4 114. Plaintiff, on behalf of himself and all others similarly situated, brings this action pursuant  
5 to California Code of Civil Procedure section 382. This action satisfies the numerosity, commonality,  
6 typicality, adequacy, predominance, and superiority requirements.

7 115. The proposed class (“Class”) is defined as: “All persons to whom the CDPH Mailing was  
8 mailed, provided, or sent for delivery.”

9 116. Plaintiff reserves the right to modify or amend the definition of the proposed Class before  
10 the Court determines whether certification is appropriate.

11 117. The Class is sufficiently numerous such that joinder of all Class members is  
12 impracticable. The proposed Class contains approximately 460 persons according to CDPH, although it  
13 is possible that additional individuals’ information was improperly accessed and/or disclosed. The Class  
14 is also ascertainable, as membership in the Class can be determined by the application of objective  
15 criteria.

16 118. The factual bases of Defendants’ misconduct are common to all Class members and  
17 represent a common thread of unlawful and illegal conduct that results in common injury to all members  
18 of the Class. Common questions of law and fact exist as to all members of the Class and predominate  
19 over questions affecting only individual Class members. These common legal and factual questions  
20 include, but are not limited to, the following:

- 21 (a) Whether Defendants implemented and maintained reasonable security practices to  
22 protect Plaintiff’s and Class members’ personal and medical information from  
23 unauthorized access, destruction, use, modification, or disclosure;
- 24 (b) Whether Defendants, their employees, agents, contractors, officers, and/or directors  
25 negligently, willfully, and/or unlawfully disclosed or permitted the unauthorized  
26 disclosure of Plaintiff’s and Class members’ personal and medical information to  
27 unauthorized persons, or are responsible for others doing so;
- 28



- 1 (c) Whether Defendants negligently, willfully, and/or unlawfully created, maintained,  
2 preserved, stored, abandoned, or disposed of Plaintiff's and Class members' personal and  
3 medical information;
- 4 (d) Whether Defendants violated California's Information Practices Act of 1977, the AIDS  
5 Public Health Records Confidentiality Act, the California Medical Information Act, and  
6 the other laws cited herein;
- 7 (e) The proper method or methods by which to measure damages, restitution, restitutionary  
8 disgorgement, or other forms of monetary relief; and
- 9 (f) The form and scope of injunctive relief to which the Class is entitled.

10 119. Plaintiff's claims are typical of the claims of other members of the Class and there is no  
11 primary defense available to Defendants that is unique to Plaintiff. Plaintiff, like all Class members, was  
12 enrolled in ADAP and/or OA-HIPP programs administered by CDPH through Thrive Tribe, had his  
13 personal and medical information disclosed to third parties as a result of Defendants' conduct without  
14 his authorization or consent, and has not received the statutory, actual, or other damages to which he is  
15 entitled under the laws set forth herein.

16 120. Plaintiff will fairly and adequately represent the interests of the Class members. Plaintiff  
17 has retained counsel with substantial experience in prosecuting complex litigation and class actions,  
18 including actions concerning the protection of the sensitive medical information of individuals living  
19 with HIV. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the  
20 Class and have the financial resources to do so. Neither Plaintiff nor his counsel has any interest adverse  
21 to or that irreconcilably and materially conflicts with those of the other Class members.

22 121. Absent a class action, most members of the Class would find the cost of litigating their  
23 claims to be prohibitive and will have no effective remedy. The class treatment of common questions of  
24 law and fact is also superior to multiple individual actions or piecemeal litigation in that it conserves the  
25 resources of the courts and litigants and promotes consistency and efficiency of adjudication. By contrast,  
26 the conduct of this action as a class action presents few management difficulties, conserves the resources  
27 of the parties and the court system, and protects the rights of each Class member by providing substantial  
28

1 benefits to all litigants and the Court. Plaintiff anticipates no difficulty in the management of this case as  
2 a class action.

3 122. Class treatment is also appropriate because Defendants have acted on grounds generally  
4 applicable to the Class, making class-wide equitable, injunctive, declaratory, and monetary relief  
5 appropriate.

## 6 **CAUSES OF ACTION**

### 7 **First Cause of Action**

#### 8 **Violation of the Information Practices Act of 1977**

9 **Cal. Civ. Code § 1798 *et seq.***

10 **(Against All Defendants)**

11 123. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

12 124. This Cause of Action is brought against all Defendants.

13 125. In adopting the Information Practices Act, the Legislature declared “that the right to  
14 privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of  
15 California and by the United States Constitution and that all individuals have a right of privacy in  
16 information pertaining to them.” (Cal. Civ. Code § 1798.1.) The Legislature found that the “right to  
17 privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal  
18 information and the lack of effective laws and legal remedies.” (*Ibid.*) Additionally, “[t]he provisions of  
19 this chapter shall be liberally construed so as to protect the rights of privacy arising under this chapter or  
20 under the Federal or State Constitution.” (Cal. Civ. Code § 1798.63.)

21 126. To fulfill these goals, the Legislature adopted Cal. Civ. Code section 1798.21, requiring  
22 agencies of the State of California to “establish rules of conduct for persons involved in the design,  
23 development, operation, disclosure, or maintenance of records containing personal information and  
24 instruct each such person with respect to such rules and the requirements of this chapter, including any  
25 other rules and procedures adopted pursuant to this chapter and the remedies and penalties for  
26 noncompliance.”

27 127. Cal. Civ. Code section 1798.21 further states that “[e]ach agency shall establish  
28 appropriate and reasonable administrative, technical, and physical safeguards to ensure the security and

1 confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity  
2 which could result in any injury.”

3 128. Similarly, Cal. Civ. Code section 1798.19 requires that “[e]ach agency when it provides  
4 by contract for the operation or maintenance of records containing personal information to accomplish  
5 an agency function, shall cause, consistent with its authority, the requirements of this chapter to be  
6 applied to those records.”

7 129. “Personal information” is defined to mean “any information that is maintained by an  
8 agency that identifies or describes an individual, including, but not limited to, his or her name, Social  
9 Security number, physical description, home address, home telephone number, education, financial  
10 matters, and medical or employment history. It includes statements made by, or attributed to, the  
11 individual.” (Cal. Civ. Code § 1798.3(a).)

12 130. Defendant Thrive Tribe agreed to, was authorized to, and did act on behalf of CDPH  
13 under contract related to the operation of the CDPH’s ADAP and OA-HIPP programs. CDPH contracted  
14 with Thrive Tribe to, among other things, enroll people living with HIV and AIDS into the ADAP and  
15 OA-HIPP programs and secure the protection of their data. CDPH’s actions and inactions constitute a  
16 violation of a mandatory duty established by statute.

17 131. Both the CDPH and Thrive Tribe are jointly and severally responsible and liable for  
18 violating the California Information Practices Act of 1977. Plaintiff “may bring a civil action against an  
19 agency whenever such agency . . . fails to comply with any other provision of this chapter, or any rule  
20 promulgated thereunder, in such a way as to have an adverse effect on an individual.” (Cal. Civ. Code  
21 § 1798.45.)

22 132. In addition, “[a]ny person, other than an employee of the state or of a local government  
23 agency acting solely in his or her official capacity, who intentionally discloses information, not otherwise  
24 public, which they know or should reasonably know was obtained from personal information maintained  
25 by a state agency . . . shall be subject to a civil action, for invasion of privacy, by the individual to whom  
26 the information pertains.” (Cal. Civ. Code § 1798.53.)

27 133. Mr. Anderson, who was acting as an agent or employee of Thrive Tribe, Evolve  
28 Healthcare, and Premier Pharmacy, improperly accessed non-public information he obtained from Thrive

1 Tribe. Mr. Anderson either knew or reasonably should have known this non-public information was being  
2 held and retained by Thrive Tribe in its capacity as an agent or contractor of CDPH, and thus would  
3 qualify as records and personal information “maintained by a state agency.” Mr. Anderson thereafter  
4 disclosed such non-public information to Mr. Goldstein, Evolve Healthcare, and Premier Pharmacy  
5 pursuant to arrangements to share such data, as set forth above.

6 134. Mr. Goldstein, Premier, and Evolve Healthcare further caused such non-public  
7 information to be disclosed in pursuit of the strategies outlined above, and/or were responsible for the  
8 acts of their agents, employees, officers, or directors in doing so. Thus, such persons are jointly and  
9 severally liable for violating the California Information Practices Act of 1977.

10 135. The injury to Plaintiff and the Class is the kind of injury that the Information Practices  
11 Act was designed to protect against, and the injury was proximately caused by (i) CDPH’s and Thrive  
12 Tribe’s failure to exercise reasonable diligence to discharge their mandatory duty to protect personal  
13 information from unauthorized disclosure, and (ii) the actions of other defendants to obtain and/or  
14 disclose that information.

15 136. Defendants’ conduct as alleged in detail above violates the California Information  
16 Practices Act of 1977 in at least the following ways:

- 17 (a) Defendants CDPH and Thrive Tribe requested and came into possession of Plaintiff’s  
18 and Class members’ personal and medical information as a state agency and contractor  
19 of that agency to accomplish the agency’s function of coordinating state programs,  
20 services, and activities relating to HIV and AIDS, and had a statutory duty to preserve  
21 the confidentiality of this information. CDPH and Thrive Tribe failed to do so.
- 22 (b) Defendants CDPH and Thrive Tribe failed to “establish appropriate and reasonable  
23 administrative, technical, and physical safeguards to ensure the security and  
24 confidentiality of records, and to protect against anticipated threats or hazards to their  
25 security or integrity which could result in any injury.”
- 26 (c) CDPH and Thrive Tribe caused, permitted, or failed to prevent the unauthorized  
27 disclosure of Plaintiff’s and Class members’ personal and medical information without  
28 first obtaining Plaintiff’s and Class members’ written authorization or consent.

1 (d) Mr. Anderson, who was an agent, employee, officer, and/or director of Evolve Healthcare  
2 and Premier Pharmacy, improperly accessed non-public information obtained from and  
3 held by Thrive Tribe that would qualify as records and personal information “maintained  
4 by a state agency,” which was thereafter disclosed to Mr. Goldstein, Evolve Healthcare,  
5 and Premier Pharmacy, all of which thereafter made additional disclosures of such data  
6 and/or were responsible for the acts of their agents, employees, officers, and directors in  
7 doing so.

8 (e) Premier Pharmacy accessed the data in question as outlined above, resulting in Plaintiff’s  
9 and other similarly situated individuals’ personal and medical information being taken  
10 without authorization.

11 137. All Defendants also permitted, were aware of, took advantage of, and/or did not stop or  
12 timely report the unauthorized intentional disclosure of protected personal information described herein,  
13 and thus are jointly and severally responsible therefor.

14 138. As a result of Defendants’ failure to comply with and/or ensure compliance with the  
15 California Information Practices Act of 1977, Plaintiff and members of the Class have suffered injury.

16 139. As Defendants disclosed, received, or conspired and aided and abetted the disclosure of  
17 such personal information, they are liable for a minimum of \$2,500 in statutory damages for each  
18 violation, any actual or special damages, including damages for mental suffering, as well as attorneys’  
19 fees and other litigation costs.

20 140. Unless and until enjoined and restrained by order of this Court, the Non-State  
21 Defendants’ wrongful conduct will continue to cause Plaintiff and the Class irreparable injury in that the  
22 personal identification information maintained by the Non-State Defendants can be disclosed to  
23 additional unauthorized persons. Plaintiff and members of the Class have no adequate remedy of law for  
24 the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiff  
25 and the Class unless enjoined. Therefore, pursuant to Cal. Civ. Code § 1798.47, Plaintiff seeks an order  
26 from this Court to prevent further unauthorized disclosures of the data.

1 **Second Cause of Action**

2 **Violation of the AIDS Public Health Records Confidentiality Act**

3 **Cal. Health & Safety Code § 121025 *et seq.***

4 **(Against All Defendants)**

5 141. Plaintiff incorporates the allegations set forth in paragraphs 1–122 as if fully set forth  
6 herein.

7 142. This Cause of Action is brought against all Defendants.

8 143. The AIDS Public Health Records Confidentiality Act provides that “[p]ublic health  
9 records relating to human immunodeficiency virus (HIV) or acquired immunodeficiency syndrome  
10 (AIDS), containing personally identifying information, that were developed or acquired by a state or local  
11 public health agency, or an agent of that agency, are confidential and shall not be disclosed, except as  
12 otherwise provided by law for public health purposes or pursuant to a written authorization by the person  
13 who is the subject of the record or by his or her guardian or conservator.” (Health & Safety Code  
14 § 121025(a).)

15 144. Under the AIDS Public Health Records and Confidentiality Act, CDPH and Thrive Tribe  
16 had an obligation to prevent the disclosure of this information to unauthorized third parties without first  
17 having written authorization to do so from Plaintiff and members of the Class. In addition, disclosure of  
18 that information without written authorization by Mr. Anderson, an agent or employee of Mr. Goldstein,  
19 Evolve Healthcare, and Premier Pharmacy, constitutes a violation of the statute, as do the subsequent  
20 disclosures set forth above.

21 145. Defendant Thrive Tribe agreed to and was authorized to act on behalf of CDPH related  
22 to the operation of the CDPH’s ADAP and OA-HIPP programs.

23 146. CDPH contracted with Thrive Tribe to, among other things, enroll individuals into  
24 CDPH’s ADAP and OA-HIPP programs.

25 147. Defendant Thrive Tribe was an agent and contractor of CDPH. As an agent of a state  
26 public health agency, Thrive Tribe is subject to the requirements of the California AIDS Public Health  
27 Records and Confidentiality Act. Defendant CDPH is also subject to the statute.

1           148. Plaintiff and the Class members entrusted Thrive Tribe and the State Defendants with  
2 individualized private health information that constituted public health records relating to HIV or AIDS  
3 and that contained personally identifying information, including their names, Social Security numbers,  
4 addresses, and/or other information that could directly or indirectly lead to the identification of such  
5 individuals. Thrive Tribe, acting in its capacity as an agent of CDPH, had a legal duty to preserve the  
6 confidentiality of the records of Plaintiff and members of the Class, as such information cannot be  
7 disclosed except as otherwise provided by law for public health purposes or pursuant to a written  
8 authorization by the person who is the subject of the record or by his or her guardian or conservator. The  
9 private health information that Plaintiff and the members of the Class entrusted to Thrive Tribe, including  
10 their status as individuals living with HIV, that Thrive Tribe disclosed thus constituted confidential  
11 “public health records” as defined by Health and Safety Code section 121035(c).

12           149. CDPH’s actions and inactions constitute a violation of a mandatory duty. The injury to  
13 Plaintiff and the class is the kind of injury that the AIDS Public Health Records Confidentiality Act was  
14 designed to protect against, and the injury was proximately caused by CDPH’s failure to discharge its  
15 mandatory duty. CDPH has failed to exercise reasonable diligence to discharge that duty. None of the  
16 disclosures of data at issue were made pursuant to Health & Safety Code section 121026.

17           150. Thrive Tribe’s improper conduct with respect to this private information made it  
18 accessible, available, viewable, and/or downloadable to unauthorized individuals. The private health  
19 information of Plaintiff and the Class that was contained in confidential public health records was  
20 improperly accessed by multiple unauthorized persons or entities as a result of Defendants’ wrongful  
21 conduct.

22           151. Mr. Anderson disclosed confidential “public health records” subject to the protections of  
23 this statute to Mr. Goldstein, Evolve Healthcare, and Premier Pharmacy as set forth above.

24           152. Mr. Goldstein, Evolve Healthcare, and Premier Pharmacy made additional unauthorized  
25 disclosures as set forth above and/or were responsible for the acts of their agents, employees, officers,  
26 and directors in doing so.

27           153. These records cannot be disclosed, except as otherwise provided by law for public health  
28 purposes or pursuant to a written disclosed absent authorization by the person who is the subject of the

1 record or by his or her guardian or conservator. These Defendants did not have written authorization from  
2 Plaintiff and Class members to access, use, disclose, or otherwise exploit such information.

3 154. As these Defendants wrongfully disclosed or permitted the disclosure of the content of a  
4 confidential public health record to a third party without written authorization and/or were responsible  
5 for the acts of their agents, employees, officers, and directors in doing so, they are subject to a civil  
6 penalty in an amount not less than five thousand dollars (\$5,000) for each violation (*i.e.*, each  
7 unauthorized disclosure, and there were multiple disclosures as set forth above), each of which is a  
8 separate and actionable offense, and not more than twenty-five thousand dollars (\$25,000) for each  
9 violation, plus court costs.

10 155. Alternatively, as these Defendants negligently disclosed or permitted the disclosure of  
11 the content of a confidential public health record to a third party without written authorization and/or  
12 were responsible for the acts of their agents, employees, officers, and directors in doing so, they are  
13 subject to a civil penalty in an amount not to exceed five thousand dollars (\$5,000) for each violation  
14 (*i.e.*, each unauthorized disclosure, and there were multiple disclosures as set forth above), each of which  
15 is a separate and actionable offense, plus court costs.

16 156. In addition, as these Defendants negligently or willfully disclosed or permitted the  
17 disclosure of the content of a confidential public health record to a third party without written  
18 authorization and/or were responsible for the acts of their agents, employees, officers, and directors in  
19 doing so, where the unauthorized disclosure resulted in economic, bodily, or psychological harm to  
20 members of the Class, Defendants are liable for all actual damages as a result of any economic, bodily,  
21 or psychological harm that is a proximate result of such acts, plus court costs.

22 **Third Cause of Action**

23 **Violation of the Confidentiality of Medical Information Act (“CMIA”)**

24 **Cal. Civ. Code § 56 *et seq.***

25 **(Against Non-State Defendants and DOES 2–25)**

26 157. Plaintiff incorporates the allegations in 1–122 as if fully set forth herein.

27 158. This Cause of Action is brought against all Defendants except the State Defendants.  
28



1           159. The Non-State Defendants and DOES 2–25 are subject to the requirements and mandates  
2 of the CMIA.

3           160. Defendant Thrive Tribe is a “Contractor” as defined by Cal. Civ. Code section 56.05(d)  
4 and/or a “Provider of Health Care” as expressed in Cal. Civ. Code section 56.06.

5           161. Defendant Evolve Healthcare is a “Contractor” as defined by Cal. Civ. Code section  
6 56.05(d) and/or a “Provider of Health Care” as expressed in Cal. Civ. Code section 56.06.

7           162. Defendant Mr. Goldstein, as the CEO, funder, director, agent, or employee of Defendants  
8 Evolve Healthcare and/or Premier Pharmacy, is responsible for ensuring these entities comply with all  
9 applicable laws and/or for the unlawful conduct described above and thus qualifies as a “provider of  
10 health care” or is otherwise a person who negligently released confidential information or records of  
11 Plaintiff and Class members.

12           163. Defendant Mr. Anderson, as an officer, director, employee, agent, and/or representative  
13 of Defendants Evolve Healthcare and/or Premier Pharmacy, is responsible for ensuring these entities  
14 comply with all applicable laws and/or for the unlawful conduct described above and thus qualifies as a  
15 “provider of health care” or is otherwise a person who negligently released confidential information or  
16 records of Plaintiff and Class members.

17           164. Defendant Premier Pharmacy is a “Contractor” as defined by Cal. Civ. Code section  
18 56.05(d), a “Pharmaceutical company” as defined by Cal. Civ. Code section 56.05(l), a “provider of  
19 health care” as defined in Cal. Civ. Code section 56.06, or is otherwise a person who negligently released  
20 confidential information or records of Plaintiff and Class members.

21           165. Plaintiff and the Class members are “Patients” as defined by Cal. Civ. Code section  
22 56.05(k).

23           166. Plaintiff’s and Class members’ personal and medical information that was the subject of  
24 the unauthorized disclosure included “medical information” as defined by Cal. Civ. Code  
25 section 56.05(j).

26           167. In violation of the CMIA, the Non-State Defendants negligently released confidential  
27 information or records concerning Plaintiff and the Class. (Cal. Civ. Code § 56.10(b).)  
28

1           168. In violation of the CMIA, the Non-State Defendants disclosed and/or used the medical  
2 information of Plaintiff and Class members without first obtaining an authorization to do so. (Cal. Civ.  
3 Code §§ 56.10(a), 56.11, 56.13.)

4           169. In violation of the CMIA, the Non-State Defendants shared, sold, used for marketing, or  
5 otherwise used medical information of Plaintiff and the Class members for a purpose not necessary to  
6 provide health care services to Plaintiff or the Class members. (Cal. Civ. Code § 56.10(d).)

7           170. In violation of the CMIA, Thrive Tribe, Mr. Anderson, and Mr. Goldstein, as employees  
8 or agents of Thrive Tribe, wrongfully used, disclosed, or permitted their employees or agents to use or  
9 disclose “medical information possessed in connection with performing administrative functions” of the  
10 OA-HIPP and ADAP programs. (Cal. Civ. Code § 56.26(a).) ADAP and OA-HIPP provide payment for  
11 health care services on behalf of HIV and AIDS patients.

12           171. In violation of the CMIA, Thrive Tribe failed to maintain, preserve, and store medical  
13 information “in a manner that preserves confidentiality of the information contained therein.” Cal. Civ.  
14 Code § 56.101(a). Electronic medical record systems are required to “protect and preserve the integrity  
15 of electronic medical information.” (*Ibid.*) Plaintiff and Class members entrusted Thrive Tribe with their  
16 private information, and, at all relevant times, Thrive Tribe had a legal duty to protect and exercise  
17 reasonable care in preserving the confidentiality of Plaintiff’s and other Class members’ personal and  
18 medical information. Thrive Tribe failed to do so.

19           172. In violation of the CMIA, Thrive Tribe’s electronic health record systems or electronic  
20 medical record systems did not protect and preserve the integrity of Plaintiff’s and Class members’  
21 medical information. (*Ibid.*)

22           173. As a direct and proximate result of the Non-State Defendants’ violations of Cal. Civ.  
23 Code section 56 *et seq.*, Plaintiff and Class members now face an increased risk of future harm and have  
24 suffered fear, anxiety, and worry caused by the unauthorized disclosure of their medical information.

25           174. None of the statutory affirmative defenses set forth in the CMIA apply to justify the Non-  
26 State Defendants’ conduct.

27           175. As a result of such violations, Plaintiff and Class members pursuant to Cal. Civ. Code  
28 section 56.36 are entitled to damages in an amount to be proven at trial, including statutory damages of

1 \$1,000 per violation per person (*i.e.*, each unauthorized disclosure, and there were multiple disclosures  
2 as set forth above), actual damages, and reasonable attorneys' fees and costs.

3 **Fourth Cause of Action**

4 **Invasion of Privacy**

5 **(Against Non-State Defendants and DOES 2–25)**

6 176. Plaintiff incorporates by reference paragraphs 1–122 as though fully stated herein.

7 177. This Cause of Action is brought against all Defendants except the State Defendants.

8 178. The right to privacy is recognized under common law of this State and also is a personal  
9 and fundamental right protected by Section 1 of Article I of the Constitution of California and by the  
10 United States Constitution in that all individuals have a right of privacy in information pertaining to them.  
11 As a result of being a CDPH contractor providing assistance to Plaintiff and the Class members with  
12 enrolling in and maintaining eligibility in CDPH's ADAP and OA-HIPP's programs, Defendant Thrive  
13 Tribe invaded or permitted the invasion of Plaintiff's and the Class members' right to privacy by allowing  
14 the unauthorized access to the personal and medical information of Plaintiff and the Class members by  
15 and to third parties and negligently maintaining the confidentiality of this information, as set forth in  
16 detail above.

17 179. The Non-State Defendants invaded Plaintiff's and the Class members' right to privacy  
18 by participating in obtaining and using the personal and medical information of Plaintiff and the Class  
19 members for their personal profit and benefit and/or by negligently maintaining the confidentiality of this  
20 data, as set forth above.

21 180. This intrusion was offensive and objectionable to Plaintiff and Class members and would  
22 be offensive and objectionable to a reasonable person of ordinary sensibilities.

23 181. This intrusion was into information that was private and is entitled to be private in that  
24 Plaintiff's and Class members' personal medical information provided to Defendant Thrive Tribe as  
25 enrollees in ADAP and OA-HIPP by contract and by law was intended to be kept confidential and  
26 protected from unauthorized disclosure.

1 182. As a proximate result of the Non-State Defendants' acts as set forth in detail above,  
2 Plaintiff's and Class members' personal and medical information was viewed, distributed, and used  
3 without prior written authorization to persons unauthorized to access such information.

4 183. Plaintiff and the Class members suffered general damages in an amount to be determined  
5 at trial according to proof.

6 184. Plaintiff and Class members are also entitled to appropriate injunctive relief.

7 185. By permitting the unauthorized access to and disclosure of Plaintiff's and the Class  
8 members' personal and medical information, including their HIV status, with a willful or conscious  
9 disregard of Plaintiff's and the Class members' right to privacy, the Non-State Defendants are guilty of  
10 oppression, fraud, or malice, thereby entitling Plaintiff and Class members to an award of exemplary  
11 damages.

### 12 **Fifth Cause of Action**

#### 13 **Negligence**

#### 14 **(Against Non-State Defendants and DOES 2–25)**

15 186. Plaintiff incorporates by reference paragraphs 1–122 as though fully stated herein.

16 187. This Cause of Action is brought against all Defendants except the State Defendants.

17 188. The Non-State Defendants had a foreseeable duty to keep Plaintiff's and Class members'  
18 private, non-public personal, medical, and health-related information private and confidential.

19 189. The Non-State Defendants had a foreseeable duty to Plaintiff and Class members to  
20 exercise reasonable care to not access Plaintiff's and Class members' non-public personal and medical  
21 information without authorization or consent and to prevent such information from being accessed by  
22 unauthorized persons without their authorization or consent. This duty included refraining from accessing  
23 or exploiting such information; creating, maintaining, testing, and/or securing any databases containing  
24 non-public personal and medical information; and ensuring that Plaintiff's and Class members' non-  
25 public personal and medical information was either not accessed by them without first obtaining  
26 authorization to do so or secured from access by unauthorized personnel, including current and former  
27 employees.  
28

1           190.    The Non-State Defendants had a foreseeable duty to Plaintiff and Class members to  
2 implement processes to detect unauthorized access to their computers or systems in a timely manner and  
3 to act upon any warnings or alerts that such computers or systems were improperly accessed.

4           191.    The Non-State Defendants had a foreseeable duty to Plaintiff and Class members to  
5 timely disclose any unauthorized access to their computers or systems. The Non-State Defendants  
6 breached each of these duties by their conduct alleged herein. As a proximate result of Defendants’ breach  
7 of such duties by engaging in the conduct described herein, Plaintiff and members of the Class have  
8 suffered, and will continue to suffer, damages and injuries for which they are entitled to be compensated.

9                                 **Sixth Cause of Action**

10                               **Violation of the Unfair Competition Law**

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

12                               **(Against Non-State Defendants and DOES 2–25)**

13           192.    Plaintiff incorporates by reference paragraphs 1–122 as though fully stated herein, except  
14 any allegations as to entitlement to damages.

15           193.    This Cause of Action is brought against all Non-State Defendants.

16           194.    The information obtained, disclosed, and/or used by the Non-State Defendants without  
17 authorization or consent identifies, relates to, describes, is reasonably capable of being associated with,  
18 or could reasonably be linked, directly or indirectly, with a particular consumer or household and thus is  
19 defined as “personal information.” The personal information of Plaintiff and Class members has an  
20 independent monetary value, depending on the amount and quality of information available, the  
21 demographics of the clients in a customer database, and whether such customers have used or reused the  
22 companies’ products or services. Such information and databases are considered property, the non-  
23 disclosure of which is protected by law, including the laws set forth above.

24           195.    Because personal information is both valuable and fungible data, the specific information  
25 provided at issue is property that, as evidenced by the entities that accessed the data without authorization,  
26 the profits to be derived from such data and the alleged purpose and profits for doing so derives an  
27 independent economic value, and from which the Non-State Defendants have derived or have attempted  
28 to derive economic value. Such information is also of value and interest to Plaintiff and Class members,

1 for which they have a cognizable claim in terms of controlling who does and who does not have access  
2 to such information. It is property with a specific definable value to the Non-State Defendants in which  
3 Plaintiff and Class members, by virtue of state and federal law, have a vested interest in its value, control,  
4 protection, and dissemination, as evidenced by the statutory references and agreements referenced herein.  
5 Plaintiff and Class members were not compensated in any way by the Non-State Defendants in exchange  
6 for the unlawful use of Plaintiff's and Class members' personal information.

7         196. Plaintiff and Class members were required to provide the above personal, medical, and  
8 financial information to Thrive Tribe in order obtain their assistance with enrolling in and maintaining  
9 eligibility in ADAP and OA-HIPP. Plaintiff and Class members' interest in such data was compromised,  
10 diminished, and deprived in whole or in part by having this information disclosed to third parties without  
11 Plaintiff's and Class members' authorization or consent who thereafter used it for their own profit,  
12 exploitation, use, and misuse. Plaintiff thereby surrendered more and/or acquired less in a transaction  
13 than he otherwise would have if the Non-State Defendants had fully informed him of the true facts. In  
14 addition, the risk that Plaintiff's and Class members' personal data will be accessed and misused by  
15 hackers and cybercriminals is immediate and very real. This results in an increased risk of identity theft  
16 or fraud, as such information can be used not only to solicit transactions, but also gives third parties the  
17 ability to target them in schemes and identity theft attacks by using this specific personal information.

18         197. Plaintiff was also injured in fact by suffering fear, anxiety, and worry caused by the  
19 unauthorized disclosure of his personal and medical information and not knowing who accessed such  
20 information and/or having to spend hours dealing with these issues related to the unauthorized disclosure  
21 of this personal and medical information. The disclosure of such personal information to Evolve  
22 Healthcare, Mr. Goldstein, Mr. Anderson, and/or Premier Pharmacy was intended for those Defendants'  
23 profit and was undertaken without Plaintiff's advance authorization or consent to do so.

24         198. Plaintiff has therefore suffered an injury in fact and lost money or property as a result of  
25 the Non-State Defendants' conduct, *inter alia*, because the personal and medical non-public information  
26 in which he has a vested interest and that he provided to Thrive Tribe solely for purposes of enrolling in  
27 the ADAP and OA-HIPP programs was unlawfully disclosed at a minimum to Evolve Healthcare,  
28 Mr. Goldstein, Mr. Anderson, and Premier Pharmacy, who did not maintain adequate controls over such

1 data. Such personal and medical information is a valuable asset that has been and can be exploited for  
2 profit and has its own independent economic value. Plaintiff would not have provided that information  
3 to Thrive Tribe had the true facts been timely disclosed. Plaintiff suffered further injury in fact by not  
4 being paid all compensation he was entitled to by statute, including the statutes set forth above.

5 199. The Non-State Defendants' conduct violates California Business and Professions Code  
6 section 17200 in the following respects:

7 (a) The Non-State Defendants' mishandling and misuse of Plaintiff's and Class members'  
8 personal and medical information, as set forth above, constitutes an unlawful business  
9 practice because the Non-State Defendants' conduct violates California Civil Code  
10 sections 56 *et seq.* and 1798 *et seq.*, California Health & Safety Code section 121025,  
11 and invasion of privacy and negligence, all as set forth in detail above;

12 (b) The Non-State Defendants' mishandling and misuse of Plaintiff's and Class members'  
13 personal and medical information, as set forth above, constitutes an unfair business  
14 practice. As the conduct at issue is not conduct directed between competitors but conduct  
15 directed at consumers, there are several tests that determine whether a practice is  
16 "unfair," which examine the practice's impact on the public balanced against the reasons,  
17 justifications, and motives of the Non-State Defendants. For example,

18 (i) does the practice offend an established public policy? Here the practices at issue  
19 offend the policies against disclosing or improperly using confidential personal  
20 medical information as reflected in the laws set forth above;

21 (ii) balancing the utility of the Non-State Defendants' conduct against the gravity of  
22 the harm created by that conduct, did the Non-State Defendants' practice cause  
23 substantial injury to Plaintiff and Class members with little to no countervailing  
24 legitimate benefit and cause harm that could not reasonably have been avoided  
25 by the consumers themselves? Such is the circumstance in this case, as there is  
26 no utility of compromising such data from consumers' perspectives, and such  
27 practices cause substantial injury to consumers by resulting in consumers losing  
28 control over such data that they could not reasonably have avoided; or

1 (iii) is the practice immoral, unethical, oppressive, unscrupulous, unconscionable, or  
2 substantially injurious to consumers? This is evidenced by the facts alleged above  
3 in terms of failing to protect such data and/or abusing such data in a manner that  
4 profits the Non-State Defendants at the expense of consumers; and

5 (c) The Non-State Defendants' failure to timely notify Plaintiff and Class members of the  
6 unauthorized disclosure at issue constitutes a fraudulent business practice, as that failure  
7 likely misled reasonable consumers impacted by the practice to believe that their personal  
8 information was secure when in fact it had apparently been compromised for profit for  
9 well over a year.

10 200. The Non-State Defendants' unlawful, unfair, and fraudulent business practices, as  
11 described above, present a continuing threat to Plaintiff and the Class and the public since the Non-State  
12 Defendants continue to maintain the medical information of Plaintiff and the Class members. Plaintiff  
13 and the Class members may have no other adequate remedy of law absent equitable relief from the Court.

14 201. Pursuant to the Business & Professions Code section 17203, Plaintiff, for himself, the  
15 members of the Class, and the benefit of the general public, seeks an Order of this Court requiring: (i) the  
16 destruction and deletion of the personal and medical information at issue that is no longer necessary to  
17 be retained by Defendants, and/or allowing Class members to direct the destruction and deletion of that  
18 information as they so choose; (ii) payment of restitution in the form of the value of any data  
19 compromised and restitutionary disgorgement of any moneys made by the Non-State Defendants off of  
20 the use of such data; and (iii) Defendants to engage in a corrective notice campaign to provide notice to  
21 Class members of the circumstances surrounding the unauthorized access and their right to request the  
22 destruction and deletion of their personal and medical information.

23 202. Plaintiff and Class members also seek the recovery of attorneys' fees and costs in  
24 prosecuting this action against the Non-State Defendants under California Code of Civil Procedure  
25 Section 1021.5 and other applicable law.



1 **PRAYER FOR RELIEF**

2 WHEREFORE, Plaintiff, individually and on behalf of the Class members, prays for judgment  
3 in favor of Plaintiff and the Class members and against Defendants as follows, as appropriate and  
4 applicable to the Causes of Action set forth above:

- 5 A. Finding that this action satisfies the prerequisites for maintenance as a class action under  
6 California Code of Civil Procedure section 382 and certifying the Class defined herein;
- 7 B. Designating Plaintiff as representative of the Class and his counsel as Class counsel;
- 8 C. Declaring Defendants' conduct in violation of California Civil Code sections 56 *et seq.*  
9 and 1798 *et seq.*, California Health & Safety Code section 121025, and other laws as set  
10 forth above, as applicable;
- 11 D. Ordering Defendants to:
- 12 i. Destroy or delete the personal and medical information at issue that is no longer  
13 necessary to be retained by Defendants, and/or allow Class members to direct the  
14 destruction and deletion of that information as they so choose; and,
  - 15 ii. Engage in a corrective notice campaign to provide notice to Class members of the  
16 circumstances surrounding the unauthorized access and their right to request the  
17 destruction and deletion of their personal and medical information;
- 18 E. Awarding Plaintiff and members of the Class compensatory, statutory, and/or exemplary  
19 damages, and/or restitution or restitutionary disgorgement, all in amounts to be  
20 determined at trial;
- 21 F. Awarding Plaintiff's counsel reasonable attorneys' fees;
- 22 G. Awarding Plaintiff's litigation taxable and non-taxable costs and litigation expenses,  
23 including expert fees;
- 24 H. Awarding pre- and post-judgment interest at the maximum rate permitted by applicable  
25 law; and
- 26 I. Granting such further relief as the Court deems just.


27 **JURY DEMANDED**

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

1 Dated: October 6, 2022

Respectfully submitted,

2 CONSUMER WATCHDOG

3  
4 By:   
5 Jerry Flanagan  
Daniel L. Sternberg

6 WHATLEY KALLAS, LLP

7  
8 By:   
9 Alan M. Mansfield

10 *Attorneys for Plaintiff*

11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

# **EXHIBIT 1**

STATE OF CALIFORNIA  
**STANDARD AGREEMENT AMENDMENT**  
 STD 213A (Rev 6/03)

Check here if additional pages are added: 1 Page(s)

Agreement Number <b>16-10356</b>	Amendment Number <b>A01</b>
Registration Number:	

1. This Agreement is entered into between the State Agency and Contractor named below:
- State Agency's Name Also known as CDPH or the State  
**California Department of Public Health**
- Contractor's Name (Also referred to as Contractor)  
**The Thrive Tribe Foundation**
2. The term of this July 1, 2016 through June 30, 2020  
 Agreement is:
3. The maximum amount of this \$ 0  
 Agreement after this amendment is: Not Applicable - Amount Solely Based on Usage
4. The parties mutually agree to this amendment as follows. All actions noted below are by this reference made a part of the Agreement and incorporated herein:

I. **Purpose of amendment:**

This amendment will replace the following exhibits in their entirety: Exhibit A, Ai, B, D, F and G.

This agreement will continue to provide AIDS Drug Assistance Program (ADAP) and adds Pre-Exposure Prophylaxis (PrEP) Assistance Program enrollment services to local health jurisdictions, as well as community based organizations, and hospitals throughout the State of California. This contract is for costs associated with the administration of the ADAP, PrEP and Health Insurance Assistance Programs. Funding is solely based on usage.


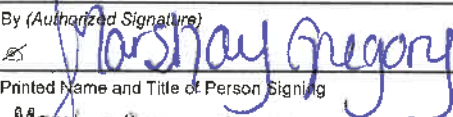
The contract term has been extended an additional year, and requirements and deliverables have been strengthened to ensure access to services and site monitoring.

- II. Certain changes made in this amendment are shown as: Text additions are displayed in **bold and underline**. Text deletions are displayed as strike through text (i.e., ~~Strike~~).

(Continued on next page)

All other terms and conditions shall remain the same.

**IN WITNESS WHEREOF, this Agreement has been executed by the parties hereto.**

CONTRACTOR		CALIFORNIA Department of General Services Use Only
Contractor's Name (If other than an individual, state whether a corporation, partnership, etc.) <b>The Thrive Tribe Foundation</b>		
By (Authorized Signature) 	Date Signed (Do not type) <b>2-27-18</b>	
Printed Name and Title of Person Signing <b>Orren Plaut, CEO</b>		
Address <b>7033 W Sunset Blvd. #201 Los Angeles, CA 90028</b>		
STATE OF CALIFORNIA		
Agency Name <b>California Department of Public Health</b>		<input checked="" type="checkbox"/> Exempt per: <b>OA Budget Act 2017</b>
By (Authorized Signature) 	Date Signed (Do not type) <b>5/7/18</b>	
Printed Name and Title of Person Signing <b>Marshay Gregory Chief Contracts Management Unit</b>		
Address <b>1616 Capitol Avenue, Suite 74.317, MS 1802, P.O. Box 997377, Sacramento, CA 95899-7377</b>		

- III. Exhibit A – Scope of Work, is replaced in its entirety with Exhibit A, A01 – Scope of Work.
- All references to Exhibit A – Scope of Work in this agreement and any exhibits hereto shall hereinafter be deemed to read Exhibit A, A01 – Scope of Work.
- IV. Exhibit A, Attachment I – Definitions of Terms, is replaced in its entirety with Exhibit A, Attachment I, A01 – Definitions of Terms.
- All references to Exhibit A, Attachment I – Definitions of Terms, in this agreement and any exhibits hereto shall hereinafter be deemed to read Exhibit A, Attachment I, A01 – Definitions of Terms.
- V. Exhibit B – Budget Detail and Payment Provisions, is replaced in its entirety with Exhibit B, A01 – Budget Detail and Payment Provisions.
- All references to Exhibit B – Budget Detail and Payment Provisions, in this agreement and any exhibits hereto shall hereinafter be deemed to read Exhibit B, A01 – Budget Detail and Payment Provisions.
- VI. Exhibit D – HIPAA Business Associate Addendum, is replaced in its entirety with Exhibit D, A01 – HIPAA Business Associate Addendum.
- All references to Exhibit D – HIPAA Business Associate Addendum, in this agreement and any exhibits hereto shall hereinafter be deemed to read Exhibit D, A01 – HIPAA Business Associate Addendum.
- VII. Exhibit F – Security Requirements, Protections, and Confidentiality Checklist, is replaced in its entirety with Exhibit F, A01 - Security Requirements, Protections, and Confidentiality Checklist.
- All references to Exhibit F– Security Requirements, Protections, and Confidentiality Checklist, in this agreement and any exhibits hereto shall hereinafter be deemed to read Exhibit F, A01 – Security Requirements, Protections, and Confidentiality Checklist.
- VIII. Exhibit G – Sample - Plan for Transporting Confidential ADAP Client Files POLICY & PROCEDURE, is replaced in its entirety with Exhibit G, A01 – Plan for Transporting Confidential ADAP Client Files.
- All references to Exhibit G – Sample - Plan for Transporting Confidential ADAP Client Files POLICY & PROCEDURE, in this agreement and any exhibits hereto shall hereinafter be deemed to read Exhibit G, A01 – Plan for Transporting Confidential ADAP Client Files.

**Exhibit A**  
Scope of Work  
July 1, 2016 through June 30, 2020

**1. Service Overview**

California Health and Safety Code (HSC) §131019 designates the California Department of Public Health (CDPH), Center for Infectious Diseases, Office of AIDS (OA) as the lead agency within the state responsible for coordinating state programs, services and activities related to Human Immunodeficiency Virus (HIV) and Acquired Immunodeficiency Syndrome (AIDS).

The Contractor agrees to provide CDPH/OA, the services described herein for the provision of the AIDS Drug Assistance Program (ADAP) and Pre-Exposure Prophylaxis Assistance Program (PrEP-AP) enrollment services, which includes the ADAP Medication Program and Health Insurance Assistance Programs, and OA's PrEP-AP. This contract agreement will be in effect for four consecutive fiscal years (FY) beginning in FY 2016-17 through FY 2019-20 (July 1, 2016 – June 30, 2020).

Refer to Exhibit A-I "Definitions of Terms" to review definitions of acronyms and other contract related terms and references.

**2. Service Location**

The services shall be performed at The Thrive Tribe Foundation, located at 7033 W. Sunset Blvd., #201, Los Angeles, CA 90028

**3. Service Hours**

The services shall be provided during normal Contractor working hours as defined by the enrollment site.

**4. Project Representatives**

A. The project representatives during the term of this agreement will be:

<b>California Department of Public Health</b>	<b>The Thrive Tribe Foundation</b>
Sandra Robinson, Branch Chief	Orren Plaut, CEO
Telephone: (916) 449-5942	Telephone: (469) 387-1737
Fax: (916) 449-5859	Fax: (818) 561-3729
Email: Sandra.Robinson@cdph.ca.gov	Email: orrenp@thethrivetribe.org

**Exhibit A**  
Scope of Work  
July 1, 2016 through June 30, 2020

B. Direct all inquiries to:

<p><b>California Department of Public Health</b></p> <p>P.O. Box 997426, MS 7704 Sacramento, CA 95899-7426</p> <p><b><u>ADAP Call Center</u></b></p> <p>Hours: Monday – Friday 8 a.m. to 5 p.m. Telephone: (844) 421-7050 Fax: (844) 421-8008</p> <p><b><u>PrEP-AP Contact</u></b> Cynthia Reed-Aguayo</p> <p>Telephone: (916) 449-5791 Fax: (916) 449-5859 Email: Cynthia.Reed-Aguayo@cdph.ca.gov</p>	<p><b>The Thrive Tribe Foundation</b></p> <p>7033 W. Sunset Blvd., #201 Los Angeles, CA90028</p> <p><b><u>Site Contact</u></b> Chris Villalobos, Associate Director</p> <p>Telephone: (469) 855-3169 Fax: (818) 561-3729 Email: chrisv@thethrivetribe.org</p>
--	---

C. Either party may make changes to the information above by giving written notice to the other party. Said changes shall not require an amendment to this agreement.

**Exhibit A**  
 Scope of Work

July 1, 2016 through June 30, 2020

**5. Services to be Performed**

**A) Major Function, Task and Activities**

The Contractor shall:

Enrollment Site Requirements	Time Line	Responsible Party	Performance Measure and/or Deliverables
<p><b>A.1. ADAP ES Contact Requirement:</b></p> <p>Maintain an ADAP Enrollment Site (ES) Contact to ensure compliance with the requirements of this contract agreement on behalf of the ADAP ES and facilitate required information exchange between the ES, CDPH/OA/ADAP, and CDPH/OA/ADAP's contracted CDPH/OA/ADAP Enrollment System (AES).</p>	<p>Throughout the life of the contract.</p>	<p>Authorized Site Administrator</p>	<p>ADAP Site Contact Name and contact information must be identified in Section 4B. Provide written notice to the assigned ADAP Advisor/PrEP-AP Advisor immediately of any changes to the ADAP ES Contact.</p>
<p><b>A.2. Nondiscrimination Requirements:</b></p> <p>Comply with the provisions as stated in Exhibit H, "Nondiscrimination Clause" (STD 17A). The ADAP ES shall not unlawfully discriminate against any employee or applicant for employment because of race, religion, color, national origin, ancestry, physical handicap, medical condition, marital status, age, sex, or sexual orientation.</p>	<p>Must be maintained through the life of the contract.</p>	<p>Authorized Site Administrator/ Agency's EEO Officer</p>	<p>Authorized Site Administrator and/or EEO Officer Name and contact information must be identified in Section 4A.</p>



**Exhibit A**  
 Scope of Work  
 July 1, 2016 through June 30, 2020

<p><b>A.3. Information Privacy and Security Requirements:</b></p> <p>All personnel conducting ADAP/PrEP-AP enrollment services must abide by all applicable laws and CDPH/OA/ADAP and PrEP-AP guidelines regarding confidentiality of ADAP and PrEP-AP client eligibility files and protected health information when accessing or submitting client data.</p> <p>i. Ensure compliance with the provisions as stated in Exhibit D, "HIPAA Business Associate Addendum (CDPH HIPAA BAA 6-16).</p> <p>ii. Ensure that all EWs employed by or volunteering at the ES are issued/assigned an Agency email address.  <i>*To ensure client confidentiality, ADAP EWs are prohibited from using a personal email address (i.e. gmail, yahoo, etc.) for ADAP related correspondence.</i></p>	<p>Must be maintained through the life of the contract.</p> <p>Contractor shall also continue to extend the protections of these provisions to protected health information upon termination or expiration of the agreement until its return or destruction.</p> <p>At the time of ADAP EW activation and throughout the life of the contract.</p>	<p>ADAP ES Contact</p> <p>Authorized Site Administrator/        Site Contact</p>	<p>Notify the assigned ADAP or PrEP-AP Advisor immediately by phone call plus email or fax when a potential breach has occurred. EWs may be deactivated if more than two potential breaches occur within a calendar year. ESs may also be deactivated if potential breaches are committed by more than two EWs in a calendar year.</p> <p>Verified when ADAP Enrollment Worker(s) (EWs) email address is provided to the assigned CDPH/OA/ADAP Advisor.</p>
--	--	--	---

**Exhibit A**  
 Scope of Work  
 July 1, 2016 through June 30, 2020

<ul style="list-style-type: none"> <li>• Ensure compliance with the provisions as stated in "Exhibit E, "Notice of Privacy Practices", and ensure that the notice is posted at the ES.</li> <li>• Review and sign the "Agreement by Employee/Contractor to Comply with Confidentiality Requirements (CDPH 8689)" form (Exhibit I).</li> <li>• Ensure that only certified ADAP EWs have access to ADAP client eligibility file information, unless otherwise authorized by law. Please refer to the following ADAP Confidentiality tables located under the Information flow charts for Community-Based Organizations, Health Care Provider, and Local Public Health Departments that pertains to your ADAP ES: <a href="https://www.cdph.ca.gov/Programs/CID/DOA/Pages/OA_adap_resourcepage.aspx">https://www.cdph.ca.gov/Programs/CID/DOA/Pages/OA_adap_resourcepage.aspx</a></li> </ul>	<p>Must be maintained through the life of the contract.</p> <p>ADAP ES Contact</p> <p>ADAP ES Contact and ADAP EW(s)</p>	<p>Indicate compliance on the "Security Requirements, Protections, and Confidentiality Checklist", Exhibit F.</p> <p>Submit completed CDPH Form 8689 form via the AES.</p>
<p>iii. EWs are required to ask a minimum of three security questions when confirming client identity from an incoming phone call prior to disclosing any PHI.</p>	<p>ADAP ES Contact and ADAP EW(s)</p>	<p>Notify the assigned ADAP Advisor immediately when a potential breach has occurred.</p>
<p>iv. EWs are prohibited from disclosing and must employ reasonable measures to protect their EW ID, AES password, or any other identifier/passcode which may compromise client confidentiality.</p>	<p>Must be maintained through the life of the contract.</p>	

**Exhibit A**  
 Scope of Work  
 July 1, 2016 through June 30, 2020

<p><b>A.4. ADAP ES Information Technology/Equipment Requirements:</b></p> <p>i. Ensure internet access and equipment and the ability to scan and upload the ADAP/PrEP-AP applicant/client eligibility documents to the AES secure enrollment system.</p>	<p>By the go-live date and to be maintained through the life of the contract.</p>	<p>Authorized Site Administrator and ADAP ES Contact</p>	<p>All client enrollments must occur electronically via the AES secure enrollment system.</p>
<p>ii. Only desktop computers are to be used to conduct ADAP enrollment services. The use of laptop computers or other hand held electronic devices are strictly prohibited for use in ADAP/PrEP-AP client enrollment.</p>	<p>By the go-live date and to be maintained through the life of the contract.</p>	<p>ADAP ES Contact</p>	<p>Indicate compliance on the "Security Requirements, Protections, and Confidentiality Checklist", Exhibit F.</p>
<p>iii. Ensure fax machines and CDPH/OA/ADAP fax/scanners are used to upload and submit ADAP/PrEP-AP applications or receive correspondence which may include confidential client information are located in a secure area.</p>	<p>By the go-live date and to be maintained through the life of the contract.</p>	<p>ADAP ES Contact</p>	<p>Indicate compliance on the "Security Requirements, Protections, and Confidentiality Checklist", Exhibit F.</p>
<p><b>A.5. Quality Requirements</b></p> <p>i. In order to ensure adequate service capacity and to maintain a high degree of customer service, enrollment sites are required to be adequately staffed to provide assistance to clients via in-person appointments, secure e-mails, or over the telephone within a reasonable time frame. Capacity assessments should be constructed from reasonable projections based on historical enrollments.</p>	<p>To be maintained throughout the life of the contract.</p>	<p>Authorized Site Administrator and ADAP ES Contact</p>	<p>Failure to maintain adequate service levels may result in OA transitioning clients to neighboring enrollment sites.           EWs/ESs whom are continuously unresponsive may be deactivated and precluded from performing ADAP enrollment services.</p>

**Exhibit A**  
 Scope of Work  
 July 1, 2016 through June 30, 2020

<p>ii. ADAP EWs and ESs will be held to quality standards and metrics. Please reference the ADAP Resource page found here <a href="https://www.cdph.ca.gov/Programs/CID/DOA/Pages/OA_ad_ap_resourcepage.aspx">https://www.cdph.ca.gov/Programs/CID/DOA/Pages/OA_ad_ap_resourcepage.aspx</a> for current year Quality Performance Metrics. EWs are required to maintain an enrollment performance level of at least 95 percent accuracy for ADAP/PrEP-AP eligibility documentation and enrollment. ESs are required to maintain a minimum performance level of 90 percent.</p> <p>CDPH/OA/ADAP will conduct secondary review on ADAP applications and a random sample size of PrEP applications. Applications with errors will be considered defective and will count against the performance level of the ADAP EW/ES. ADAP EW/ES quality will be factored by dividing the number of defective applications by the total number of applications processed.</p>	<p>To be maintained through the life of the contract.</p>	<p>Authorized Site Administrator and ADAP ES Contact</p>	<p>CDPH/OA/ADAP will continuously monitor performance levels throughout the life of the contract. The first year following the deployment of the AES will serve as a transition period during which OA will concentrate on evaluation and providing technical assistance.</p> <p>If after the first quarter following the initial one year transition period, an ADAP EW(s)/ES has an error rate that exceeds the quality standard, the Site Contact must submit a Corrective Action Plan to the ADAP and/or PrEP Advisor for approval within 30 days of the finding.</p> <p>If an ADAP EW(s)/ ES remains deficient for a second consecutive quarter, CDPH/OA/ADAP may suspend the EW(s)/ES for inaccurate ADAP/PrEP-AP applications processed during the quarter.</p> <p>If an ADAP EW(s)/ES remains deficient for a third consecutive quarter, the EW(s)/ES may be deactivated and will no longer be allowed to perform ADAP/PrEP-AP enrollment.</p>
---	---	--	--

**Exhibit A**  
 Scope of Work  
 July 1, 2016 through June 30, 2020

<p><b>A.6. Conduct Requirements:</b></p> <p>ADAP EWs are required to conduct themselves with a high degree of professionalism and integrity. Site Contacts are required to ensure that no ADAP EW is employed by, nor receives any financial compensation (including gifts or any other type of incentive) from a participating ADAP pharmacy and that no ADAP/PrEP-AP client enrollment is conducted at any participating ADAP pharmacy location.</p> <p>Additional examples of misconduct include, but are not limited to:</p> <ul style="list-style-type: none"> <li>i. Knowingly and willfully enrolling clients with inaccurate or false documentation.*</li> <li>ii. Insubordination and/or non-compliance with CDPH/OA/ADAP staff requests.</li> <li>iii. Verbally abusive or use of derogatory language.</li> <li>iv. Unresponsive to CDPH/OA/ADAP staff and/or client inquiries.</li> <li>v. Conducting unauthorized off-site ADAP/PrEP-AP enrollment.</li> <li>vi. Transporting files without having a transportation plan approved by CDPH/OA/ADAP staff.</li> <li>vii. Violating or otherwise not adhering to any requirement stipulated in this scope of work.</li> </ul> <p>* Knowingly providing inaccurate or false documentation may be in violation of various Penal Code laws and may be subject to violations of the California False Claims Act, which prohibits any person or entity from knowingly making or using a false statement or document to obtain money, property, or services from the State. (See California Government Code section 12650 et. seq.)</p>	<p>To be maintained through the life of the contract.</p>	<p>ADAP ES          Contact and          EW(s)</p>	<p>Notify the ADAP/PrEP-AP Advisor when instances of misconduct are identified.</p> <p>Site Contacts may be required to submit a Corrective Action Plan.</p> <p>CDPH/OA/ADAP staff to address occurrences of misconduct.</p> <p>EWs who engage in misconduct may be subject to temporary or permanent suspension of ADAP EW status.</p>
--	---	--	---

**Exhibit A**  
 Scope of Work  
 July 1, 2016 through June 30, 2020

<p><b>A.7. Training and Technical Assistance Requirements:</b></p> <p>i. Ensure all new ADAP EWs have successfully completed new ADAP EW training provided by CDPH/OA/ADAP prior to enrolling or re-certifying ADAP/PrEP-AP clients.</p> <p>ii. Ensure all existing and new enrollment workers complete training on the AES.</p>	<p>To be maintained through the life of the contract.</p>	<p>ADAP ES Contact</p>	<p>Report to the assigned ADAP/PrEP-AP Advisor, site staff who will be registering for required ADAP EW trainings.</p>
<p>iii. Ensure compliance with the requirements written in the ADAP "California State ADAP Guidelines," "California State PrEP-AP Guidelines" and ADAP Management Memos.</p>	<p>To be maintained through the life of the contract.</p>	<p>ADAP ES Contact and ADAP EW(s)</p>	<p>Notify ADAP EWs to recertify 30 days prior to the recertification end date.</p>
<p>iv. Ensure existing ADAP EWs maintain active status by participating in required annual recertifying ADAP EW trainings and/or other required ad hoc trainings provided by CDPH/OA/ADAP in order to maintain ADAP certification to continue conducting ADAP/PrEP-AP enrollment functions.</p>	<p>To be maintained through the life of the contract.</p>	<p>ADAP ES Contact</p>	<p>Must ensure ADAP ES participation for 90 percent of these calls. Must contact the ADAP Advisor, if unable to participate on a call to discuss the topics covered.</p>
<p>v. Ensure the ADAP ES has representation/participation on all monthly CDPH/OA ADAP EW calls.</p>	<p>Monthly through the life of the contract.</p>	<p>ADAP ES Contact</p>	<p></p>

**Exhibit A**  
 Scope of Work  
 July 1, 2016 through June 30, 2020

<p><b>A.8. ADAP Enrollment Tracking Requirements:</b></p> <ul style="list-style-type: none"> <li>i. Ensure all ADAP EWs are identified and have a site specific ADAP EW ID number issued by the CDPH/OA/ADAP AES.</li> <li>ii. Report any changes in site specific ADAP EWs' status (e.g., job duties, relocation, separation, etc.) that will alter the ADAP EW(s) ability to enroll clients, including the de-activation of any ADAP EW ID numbers.</li> </ul>	<p>To be maintained through the life of the contract.</p> <p>Within 24 hours of the change.</p>	<p>ADAP ES Contact</p> <p>ADAP ES Contact</p>	<p>This site specific ADAP EW ID number may only be used by the ADAP EW to whom it is assigned for enrollment activities at this site.</p> <p>Report addition/deletion/changes to ADAP EW(s) to the CDPH/OA/ADAP EBM and/or the assigned ADAP/PrEP-AP Advisor.</p>
<p><b>A.9. Transportation Plan Requirements:</b></p> <p>Ensure that no ADAP/PrEP-AP client eligibility documentation, records, files, etc., will be transported to or from the ADAP ES.</p> <p>Exception to this restriction may be approved by CDPH/OA for the following reasons:</p> <ul style="list-style-type: none"> <li>i. Client disability; or,</li> <li>ii. Remote distance requires ADAP EW to meet with client outside of the ADAP ES; or,</li> <li>iii. The entire ADAP ES is moving to a new address/location.</li> </ul> <p>Ensure that no ADAP/PrEP-AP client enrollment files will be transported until CDPH/OA/ADAP provides <u>written approval</u> of the site's specific transportation plan.</p>	<p>To be maintained through the life of the contract.</p> <p>30 days prior to the need for transporting any ADAP client enrollment documents/files.</p>	<p>ADAP ES Contact</p> <p>ADAP ES Contact</p>	<p>See "Plan for Transporting Confidential ADAP Client Files", Exhibit G.</p> <p>Submit a written request to the assigned ADAP/PrEP-AP Advisor which justifies the necessity for transporting ADAP or PrEP-AP client enrollment document/files. The request must also identify the specific procedure to be followed to safeguard the confidentiality of the ADAP/PrEP-AP client documents being transported, as well as who will be responsible/accountable for site's specific procedure(s). See "Plan for Transporting Confidential ADAP Client Files", Exhibit G.</p>

**Exhibit A**  
 Scope of Work  
 July 1, 2016 through June 30, 2020

<p><b>A.10. Administrative Requirements</b></p> <ul style="list-style-type: none"> <li>i. Notify the assigned ADAP Advisor if the site wishes to change from an open site (one which serves any individual who wishes to enroll) to a closed site (one which serves only agency-affiliated individuals) or vice versa.</li> <li>ii. Notify the assigned ADAP/PrEP-AP Advisor if the site plans to no longer provide ADAP/PrEP-AP enrollment services.</li> </ul>	<p>ADAP ES Contact</p>	<p>Provide at least 30-days' notice for the requested change of status.</p> <p>Within at least 60 days of the site deactivation date.</p>	<p>Written Request required (may be submitted by email) to ADAP/PrEP-AP Advisor.</p> <p>Written Notification required (may be submitted by email) and submission of an ADAP/PrEP-AP transportation plan to the site's designated ADAP Advisor assuring the secure transfer of hard copy ADAP/PrEP-AP client files. See page 1, item 1) Service Overview, paragraph 3.</p>
<p><b>A.11. ADAP Fiscal Requirements</b></p> <ul style="list-style-type: none"> <li>i. Ensure ADAP funds are used exclusively to cover costs related to ADAP in accordance with Health and Safety Code §120956(b).</li> <li>ii. Ensure compliance with the federal HRSA Ryan White HIV/AIDS Program requirements, polices, and National Monitoring Standards.</li> <li>iii. Ensure funds received from OA are not used for unallowable expenses as defined by the Ryan White National Monitoring Standards.</li> </ul>	<p>ADAP ES Contact/ Authorized Agency Administrator</p>	<p>To be maintained through the life of the contract.</p> <p>Within five business days of request.</p>	<p>Within five business days, upon request, submit to OA for review budget and expense reports with sufficient detail to ensure compliance with section A.11.</p> <p>In the event of an audit or upon request by CDPH, ESs must be able to adequately show that these contractual requirements have been met.</p>



**Exhibit A**  
 Scope of Work  
 July 1, 2016 through June 30, 2020

<p><b>A.12. PrEP Fiscal Requirements</b></p> <ul style="list-style-type: none"> <li>i. Ryan White funds are prohibited for the use of PrEP enrollment services.</li> <li>ii. EWs who conduct PrEP enrollment are precluded from being 100 percent funded by Ryan White funds.</li> </ul>	<p>To be maintained through the life of the contract.  Within five business days.</p>	<p>ADAP ES Contact/ Authorized Agency Administrator</p>	<p>Within 15 business days, upon request, ESs are required to submit documentation of all EWs performing PrEP enrollment with a budget detail indicating how each EW is funded.</p>
<p><b>A.13. Auditing Requirements</b></p> <ul style="list-style-type: none"> <li>i. Facilitate CDPH/OA/ADAP site visit requests, including but not limited to receiving or providing required documentation/information as requested by the assigned ADAP/PrEP-AP Advisor. Act as liaison between the site, ADAP/PrEP-AP Advisor, ADAP EW(s), and LHJ Coordinator (if applicable) in activities related to the site visit.</li> </ul>	<p>As needed during normal working hours.</p>	<p>ADAP Site Contact/Authorized Agency Administrator</p>	<p>Respond to written notifications and requests for information initiated by CDPH/OA/ADAP personnel.</p>
<ul style="list-style-type: none"> <li>ii. Ensure that CDPH/OA/ADAP staff, authorized CDPH/OA/ADAP representatives and/or other state and federal agencies are granted access to all ADAP client eligibility files and any other documentation related to this contract agreement for audit purposes.</li> </ul>	<p>As needed during normal working hours.  Within five business days.</p>	<p>ADAP Site Contact/Authorized Agency Administrator</p>	<p>Within five business days, respond to written and in-person requests for ADAP client files made by CDPH/OA/ADAP personnel.</p>
<ul style="list-style-type: none"> <li>iii. Develop and submit required Corrective Action Plan (CAP) when required based on results of ADAP site visit/federal or state program audit.</li> </ul>	<p>As needed.</p>	<p>ADAP Site Contact/Authorized Agency Administrator</p>	<p>CAP is to be submitted to the assigned ADAP/PrEP-AP Advisor by the timeframe identified in the letter indicating the CAP is required.</p>

**Exhibit A**  
 Scope of Work  
 July 1, 2016 through June 30, 2020

<p>iv. Maintain hard copy ADAP/PrEP-AP client files/records, created prior to July 1, 2016 for four years (the current year, plus three prior years)</p>	<p>To be maintained through the life of the contract.</p>	<p>ADAP ES Contact</p>	<p>As needed, records will be made available to view within the timeframe provided by the federal or state auditors.           At contract termination or expiration, Protected Health Information must be returned or retained in accordance with Exhibit D, "HIPAA Business Associate Addendum (CDPH HIPAA BAA 6-16)".</p>
<p><b>A.14. Grievance Requirements</b></p> <p>i. Ensure that ADAP/PrEP-AP clients are made aware of, and have access to, the CDPH/OA/ADAP Grievance procedures, and form as outlined in the California State ADAP/PrEP-AP Guidelines.</p>	<p>Upon initial and annual re-enrollments of ADAP clients and annual re-enrollment of PrEP-AP clients.</p>	<p>ADAP ES Contact and/or ADAP/PrEP-AP EW(s)</p>	<p>CDPH/OA/ADAP will verify, via review of the ADAP/PrEP-AP Client Satisfaction Survey.</p>
<p>ii. Upon client request, assist ADAP/PrEP-AP clients in the completion and submission of an ADAP/PrEP-AP grievance form and related documents. Assistance may also include providing the mailing address and contact information for ADAP/PrEP-AP Advisors and/or other CDPH/OA/ADAP Contractors, and/or the submission of the completed grievance form and related documents to CDPH/OA/ADAP.</p>	<p>As needed.</p>	<p>ADAP/PrEP-AP ES Contact and/or ADAP/PrEP-AP EW(s)</p>	<p>Notify the assigned ADAP/PrEP-AP Advisor immediately if assistance is needed with the CDPH/OA/ADAP/PrEP-AP grievance process.</p>

**Exhibit A**  
 Scope of Work  
 July 1, 2016 through June 30, 2020

<p><b>A.15. Performance Requirements</b></p> <ul style="list-style-type: none"> <li>i. Enrollment workers are required to vigorously pursue enrollment into health care coverage for which clients may be eligible (e.g., Medicaid, Medicare, employer-sponsored health insurance coverage, and/or other private health insurance to comply with federal and state payer of last resort requirements.</li> <li>iii. EWs are required to proactively conduct outreach to clients, by utilizing the AES dashboard to identify clients who have an eligibility expiration date within 30 days. EWs must document the client outreach in the case notes.</li> </ul>	<p>To be maintained through the life of the contract.</p>	<p>ADAP ES          Contact and/or ADAP/PrEP-AP EW(s)</p>	<p>Upon initial enrollment and annual re-enrollment. Enrollment workers are required to assess client's eligibility for other third-party coverage based on eligibility documents provided. All eligible individuals must apply.</p> <p>Outreach attempts and any client interaction as a result of said outreach must be clearly documented in the client case notes available through AES.</p>
---	---	---	--

**Exhibit A, Attachment I**  
Definition of Terms

- i. AIDS Drug Assistance Program (ADAP) – Established in 1987 to help ensure that eligible, HIV positive uninsured and under-insured individuals have access to medication on the ADAP formulary through the Medication Program and Health Insurance Assistance Programs. ADAP provides medication, premium payment, and medical out of pocket payment assistance.
- ii. ADAP Advisor – Office of AIDS ADAP staff assigned to a Local Health Jurisdiction or ADAP Enrollment Site for monitoring and technical assistance.
- iii. Enrollment Worker (EW) – Enrollment Site staff certified to provide enrollment services for ADAP and the Pre-Exposure Prophylaxis Assistance Program (PrEP-AP). EWs will have access to ADAP/PrEP-AP enrollment data.
- iv. Enrollment Site (ES) - A public health department, clinic, community based organization (CBO), or local government agency where an individual can apply for ADAP or PrEP-AP services.
- v. Enrollment Site Contact – Ensures the requirements of this contract agreement are adhered to, including but not limited to the participation in monthly EW calls. Act as the primary contact for OA, the OA service contractors, and Enrollment Site staff.
- vi. ADAP Enrollment System (AES) – ADAP's online system used for enrolling clients in ADAP and the PrEP-AP.
- vii. California Department of Public Health (CDPH) – is the lead agency in California providing detection, treatment, prevention and surveillance of public health issues.
- viii. Closed Site – An enrollment site that only serves applicants/clients associated with their entity.
- ix. Community Based Organization (CBO) – Non-profit 501 (3)(c) entities that operate within a single local community.
- x. Fiscal Year (FY) – July 1 through June 30.
- xi. Contractor – An approved enrollment site managed by a non-profit organization to provide ADAP/PrEP-AP enrollment services.
- xii. Insurance Benefits Manager (IBM) – Service contractor that manages and processes health insurance premium payments for clients enrolled in both ADAP's Medication Program and Insurance Assistance Programs.
- xiii. Local Health Jurisdiction (LHJ) – One of 58 counties and three cities (Pasadena, Long Beach, and Berkeley) in the state of California.
- xiv. Medical Benefits Manager (MBM) – Service contractor that manages and processes outpatient medical out of pocket payments for clients enrolled in ADAP's Insurance

**Exhibit A, Attachment I**  
Definition of Terms

Assistance Programs and approved PrEP related medical costs for clients enrolled in the PrEP-AP.

- xv. Office of AIDS (OA) – Has lead responsibility for coordinating state programs, services, and activities relating to HIV/AIDS as designated by California Health and Safety Code Section 131019.
- xvi. OA Health Insurance Premium Payment (OA-HIPP) – Pays for health insurance premiums and medical out of pocket costs for eligible clients co-enrolled in ADAP's Medication Program.
- xvii. OA Medicare Part D Premium Payment Program – Pays for Medicare Part D premiums for clients co-enrolled in ADAP's Medication Program.
- xviii. Open Site – An enrollment site that serves all CDPH medication assistance applicants/clients.
- xix. Pharmacy Benefits Manager (PBM) – Service contractor administering the ADAP statewide pharmacy network and providing pharmaceutical services for ADAP and PrEP-AP clients.
- xx. Pre-Exposure Prophylaxis Assistance Program (PrEP) Advisor - Office of AIDS staff assigned to provide technical assistance associated with PrEP- AP.
- xxi. PrEP-AP – PrEP-AP will cover 1) costs for HIV PrEP-related medical services for uninsured individuals who are enrolled in a drug manufacturer's PrEP medication assistance program, and 2) for insured individuals, both of the following: (a) the cost of medication copays, coinsurance, and deductibles for the prevention of HIV infection after the individual's insurance is applied and, if eligible, after the drug manufacturer's medication assistance program's contributions are applied, and b) medical copays, coinsurance, and deductibles for PrEP-related medical services.

**Exhibit B**  
Budget Detail and Payment Provisions

**1. Payments**

- A. In no event shall CDPH/OA/ADAP pay the Contractor for services performed prior to the commencement date or after the expiration of this Agreement.
- B. For services satisfactorily rendered, CDPH/OA/ADAP agrees to compensate the Contractor for actual services provided in accordance with the amounts specified in Exhibit B, Section E., Amounts Payable.
- C. Payments shall be processed by CDPH/OA/ADAP no later than the end of the quarter dates noted below.

First Quarter:                      July 1 – September 30  
Payment no later than:              November 30

Second Quarter:                     October 1 – December 31  
Payment no later than:              February 28

Third Quarter:                        January 1 – March 31  
Payment no later than:              May 31

Fourth Quarter:                      April 1 – June 30  
Payment no later than:              August 31

(FINAL) Supplemental:              July 1 – June 30  
Payment no later than:              August 31

D. Payments shall:

- 1) Be calculated based on current ADAP and PrEP-AP client enrollment data as provided by the ADAP Enrollment System to determine the number of ADAP/PrEP-AP services provided at each enrollment site.
- 2) Identify the payment period and/or performance period covered.
- 3) Itemize ADAP/PrEP-AP services for the payment period in the same level of detail as indicated in Section E Amounts Payable. Subject to the terms of this agreement, payment will only be made for those services expressly identified in this agreement as approved by CDPH/OA/ADAP.

E. Amounts Payable

All ADAP enrollment sites with a minimum of one ADAP or PrEP-AP enrollment per fiscal year (FY) will receive a floor amount with additional payment(s) per FY for performing the following ADAP/PrEP-AP services complete with all required forms and verifying documentation. Enrollment sites will be paid a fee for services performed.

The following documents and any subsequent updates are not attached, but are incorporated herein and made a part hereof by this reference. CDPH will maintain on

**Exhibit B**  
**Budget Detail and Payment Provisions**

file, all documents referenced herein and any subsequent updates, as required by program directives. CDPH shall provide the Contractor with copies of said documents and any periodic updates thereto, under separate cover.

1) ADAP Resource Page found here:  
[https://www.cdph.ca.gov/Programs/CID/DOA/Pages/OA\\_adap\\_resourcepage.aspx](https://www.cdph.ca.gov/Programs/CID/DOA/Pages/OA_adap_resourcepage.aspx)

**2. Budget Contingency Clause**

- A. It is mutually agreed that if the Budget Act of the current year and/or any subsequent years covered under this Agreement does not appropriate sufficient funds for the program, this Agreement shall be of no further force and effect. In this event, the State shall have no liability to pay any funds whatsoever to the Contractor, or to furnish any other considerations under this Agreement and Contractor shall not be obligated to perform any provisions of this Agreement.
- B. If funding for any FY is reduced or deleted by the Budget Act for purposes of this program, the State shall have the option to either cancel this Agreement with no liability occurring to the State, or offer an agreement amendment to the Contractor to reflect the reduced amount.
- C. In the event of early termination or cancellation, the Contractor shall be entitled to compensation for services performed satisfactorily under this agreement and expenses incurred up to the date of termination or cancellation and any non-cancelable obligations incurred in support of this agreement.

**3. Prompt Payment Clause**

Payment will be made in accordance with, and within the time specified in, Government Code Chapter 4.5, commencing with Section 927.

**4. Timely Final Payment**

- A. Final payment shall be processed no more than *sixty (60)* calendar days following the expiration or termination date of this agreement, unless a later or alternate deadline is agreed to in writing by the program contract manager.
- B. CDPH/OA/ADAP shall make payment to the Contractor quarterly in arrears for costs associated with the provision of ADAP enrollment services at the ADAP Enrollment Site in the local health jurisdiction (LHJ), under this contract agreement. Payment to the Contractor will be contingent upon receipt and execution of this contract agreement and the provision of ADAP/PrEP-AP enrollment services (as verified by CDPH/OA/ADAP through the AES data).
- C. This contract agreement is subject to any additional restrictions, limitations, or conditions enacted by the Congress or the State Legislature, which may affect the provisions, terms, or funding of this contract agreement in any manner.

**Exhibit B**  
Budget Detail and Payment Provisions

**5. Recovery of Overpayments**

- A. Contractor agrees that payments based upon the terms of this agreement or an audit finding and/or an audit finding that is appealed and upheld, will be recovered by CDPH/OA/ADAP by CDPH/OA/ADAP withholding payments or withholding a portion of payment for services performed until the amount of overpayment has been resolved.

If the Contractor has filed a valid appeal regarding the report of audit findings, recovery of the overpayments will be deferred until a final administrative decision on the appeal has been reached.



Exhibit D  
HIPAA Business Associate Addendum

**I. Recitals**

- A. The underlying contract (Agreement), to which this HIPAA Business Associate Addendum is attached to and made a part of, has been determined to constitute a business associate relationship under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (the HITECH Act), 42 U.S.C. section 17921 et seq., and their implementing privacy and security regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations").
- B. The Department of Public Health ("CDPH") wishes to disclose to Business Associate certain information pursuant to the terms of the Agreement, some of which may constitute Protected Health Information ("PHI"), including protected health information in electronic media ("ePHI"), under federal law, and personal information ("PI") under state law.
- C. As set forth in the Agreement, Contractor, here and after, is the Business Associate of CDPH acting on CDPH's behalf and provides services, arranges, performs or assists in the performance of functions or activities on behalf of CDPH and creates, receives, maintains, transmits, uses or discloses PHI and PI. CDPH and Business Associate are each a party to the Agreement and are collectively referred to as the "parties."
- D. The purpose of this Addendum is to protect the privacy and security of the PHI and PI that may be created, received, maintained, transmitted, used or disclosed pursuant to the Agreement, and to comply with certain standards and requirements of HIPAA, the HITECH Act and the HIPAA regulations, including, but not limited to, the requirement that CDPH must enter into a contract containing specific requirements with Contractor prior to the disclosure of PHI to Contractor, as set forth in 45 CFR Parts 160 and 164 and the HITECH Act.
- E. The terms used in this Addendum, but not otherwise defined, shall have the same meanings as those terms have in the HIPAA regulations. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.

**II. Definitions**

- A. Breach shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- B. Business Associate shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- C. Covered Entity shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- D. Electronic Health Record shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C Section 17921 and implementing regulations.
- E. Electronic Protected Health Information (ePHI) means individually identifiable health information transmitted by electronic media or maintained in electronic media, including but not limited to electronic media as set forth under 45 CFR section 160.103.
- F. Individually Identifiable Health Information means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer

Exhibit D  
HIPAA Business Associate Addendum

or health care clearinghouse, and relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual, as set forth under 45 CFR section 160.103.

- G. Privacy Rule shall mean the HIPAA Regulation that is found at 45 CFR Parts 160 and 164.
- H. Personal Information shall have the meaning given to such term in California Civil Code sections 1798.3 and 1798.29..
- I. Protected Health Information means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth under 45 CFR section 160.103.
- J. Required by law, as set forth under 45 CFR section 164.103, means a mandate contained in law that compels an entity to make a use or disclosure of PHI that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.
- K. Secretary means the Secretary of the U.S. Department of Health and Human Services ("HHS") or the Secretary's designee.
- L. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or PI, or confidential data that is essential to the ongoing operation of the Business Associate's organization and intended for internal use; or interference with system operations in an information system.
- M. Security Rule shall mean the HIPAA regulation that is found at 45 CFR Parts 160 and 164.
- N. Unsecured PHI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. section 17932(h), any guidance issued pursuant to such Act and the HIPAA regulations.

### III. Terms of Agreement

#### A. Permitted Uses and Disclosures of PHI by Business Associate

***Permitted Uses and Disclosures.*** Except as otherwise indicated in this Addendum, Business Associate may use or disclose PHI only to perform functions, activities or services specified in the Agreement, for, or on behalf of CDPH, provided that such use or disclosure would not violate the HIPAA regulations, if done by CDPH. Any such use or disclosure must, to the extent practicable, be limited to the limited data set, as defined in 45 CFR section 164.514(e)(2), or, if needed, to the minimum necessary to accomplish the intended purpose of such use or disclosure, in compliance with the HITECH Act and any guidance issued pursuant to such Act, and the HIPAA regulations.

Exhibit D  
HIPAA Business Associate Addendum

1. **Specific Use and Disclosure Provisions.** Except as otherwise indicated in this Addendum, Business Associate may:
  - a. **Use and disclose for management and administration.** Use and disclose PHI for the proper management and administration of the Business Associate provided that such disclosures are required by law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware that the confidentiality of the information has been breached.
  - b. **Provision of Data Aggregation Services.** Use PHI to provide data aggregation services to CDPH. Data aggregation means the combining of PHI created or received by the Business Associate on behalf of CDPH with PHI received by the Business Associate in its capacity as the Business Associate of another covered entity, to permit data analyses that relate to the health care operations of CDPH.

**B. Prohibited Uses and Disclosures**

1. Business Associate shall not disclose PHI about an individual to a health plan for payment or health care operations purposes if the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the individual requests such restriction, in accordance with 42 U.S.C. section 17935(a) and 45 CFR section 164.522(a).
2. Business Associate shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of CDPH and as permitted by 42 U.S.C. section 17935(d)(2).

**C. Responsibilities of Business Associate**

Business Associate agrees:

1. **Nondisclosure.** Not to use or disclose Protected Health Information (PHI) other than as permitted or required by the Agreement or as required by law.
2. **Safeguards.** To implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI, including electronic PHI, that it creates, receives, maintains, uses or transmits on behalf of CDPH, in compliance with 45 CFR sections 164.308, 164.310 and 164.312, and to prevent use or disclosure of PHI other than as provided for by the Agreement. Business Associate shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of 45 CFR section 164, subpart C, in compliance with 45 CFR section 164.316. Business Associate shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Business Associate's operations and the nature and scope of its activities, and which incorporates the requirements of section 3, Security, below. Business Associate will provide CDPH with its current and updated policies.
3. **Security.** To take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:

Exhibit D  
HIPAA Business Associate Addendum

- a. Complying with all of the data system security precautions listed in Attachment A, the Business Associate Data Security Requirements;
- b. Achieving and maintaining compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164), as necessary in conducting operations on behalf of CDPH under the Agreement;
- c. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III - Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and
- d. In case of a conflict between any of the security standards contained in any of these enumerated sources of security standards, the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI from unauthorized disclosure. Further, Business Associate must comply with changes to these standards that occur after the effective date of the Agreement.
- e. Business Associate shall designate a Security Officer to oversee its data security program who shall be responsible for carrying out the requirements of this section and for communicating on security matters with CDPH.

**D. *Mitigation of Harmful Effects.*** To mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate or its subcontractors in violation of the requirements of this Addendum.

**E. *Business Associate's Agents and Subcontractors.***

1. To enter into written agreements with any agents, including subcontractors and vendors, to whom Business Associate provides PHI or PI received from or created or received by Business Associate on behalf of CDPH, that impose the same restrictions and conditions on such agents, subcontractors and vendors that apply to Business Associate with respect to such PHI and PI under this Addendum, and that comply with all applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations.
2. In accordance with 45 CFR section 164.504(e)(1)(ii), upon Business Associate's knowledge of a material breach or violation by its subcontractor of the agreement between Business Associate and the subcontractor, Business Associate shall:
  - a. Provide an opportunity for the subcontractor to cure the breach or end the violation and terminate the agreement if the subcontractor does not cure the breach or end the violation within the time specified by CDPH; or
  - b. Immediately terminate the agreement if the subcontractor has breached a material term of the agreement and cure is not possible.

**F. *Availability of Information to CDPH and Individuals.*** To provide access and information:

1. To provide access as CDPH may require, and in the time and manner designated by CDPH (upon reasonable notice and during Business Associate's normal business hours) to PHI in a Designated Record Set, to CDPH (or, as directed by CDPH), to an Individual, in accordance with 45 CFR section 164.524. Designated Record Set means the group of records maintained for CDPH that

Exhibit D  
HIPAA Business Associate Addendum

includes medical, dental and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for CDPH health plans; or those records used to make decisions about individuals on behalf of CDPH. Business Associate shall use the forms and processes developed by CDPH for this purpose and shall respond to requests for access to records transmitted by CDPH within fifteen (15) calendar days of receipt of the request by producing the records or verifying that there are none.

2. If Business Associate maintains an Electronic Health Record with PHI, and an individual requests a copy of such information in an electronic format, Business Associate shall provide such information in an electronic format to enable CDPH to fulfill its obligations under the HITECH Act, including but not limited to, 42 U.S.C. section 17935(e).
  3. If Business Associate receives data from CDPH that was provided to CDPH by the Social Security Administration, upon request by CDPH, Business Associate shall provide CDPH with a list of all employees, contractors and agents who have access to the Social Security data, including employees, contractors and agents of its subcontractors and agents.
- G. Amendment of PHI.** To make any amendment(s) to PHI that CDPH directs or agrees to pursuant to 45 CFR section 164.526, in the time and manner designated by CDPH.
- H. Internal Practices.** To make Business Associate's internal practices, books and records relating to the use and disclosure of PHI received from CDPH, or created or received by Business Associate on behalf of CDPH, available to CDPH or to the Secretary of the U.S. Department of Health and Human Services in a time and manner designated by CDPH or by the Secretary, for purposes of determining CDPH's compliance with the HIPAA regulations. If any information needed for this purpose is in the exclusive possession of any other entity or person and the other entity or person fails or refuses to furnish the information to Business Associate, Business Associate shall so certify to CDPH and shall set forth the efforts it made to obtain the information.
- I. Documentation of Disclosures.** To document and make available to CDPH or (at the direction of CDPH) to an Individual such disclosures of PHI, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of PHI, in accordance with the HITECH Act and its implementing regulations, including but not limited to 45 CFR section 164.528 and 42 U.S.C. section 17935(c). If Business Associate maintains electronic health records for CDPH as of January 1, 2009, Business Associate must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after January 1, 2014. If Business Associate acquires electronic health records for CDPH after January 1, 2009, Business Associate must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after the date the electronic health record is acquired, or on or after January 1, 2011, whichever date is later. The electronic accounting of disclosures shall be for disclosures during the three years prior to the request for an accounting.
- J. Breaches and Security Incidents.** During the term of the Agreement, Business Associate agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:
1. **Notice to CDPH.** (1) To notify CDPH **immediately by telephone call plus email or fax** upon the discovery of a breach of unsecured PHI or PI in electronic media or in any other media if the PHI or PI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon the discovery of a suspected security incident that involves data provided to CDPH by the

Exhibit D  
HIPAA Business Associate Addendum

Social Security Administration. (2) To notify CDPH **within 24 hours by email or fax** of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI in violation of the Agreement and this Addendum, or potential loss of confidential data affecting the Agreement. A breach shall be treated as discovered by Business Associate as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Business Associate.

Notice shall be provided to the CDPH Program Contract Manager, the CDPH Privacy Officer and the CDPH Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, notice shall be provided by calling the CDPH ITSD Service Desk. Notice shall be made using the "CDPH Privacy Incident Report" form, including all information known at the time. Business Associate shall use the most current version of this form, which is posted on the CDPH Privacy Office website ([www.CDPH.ca.gov](http://www.CDPH.ca.gov)),

Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI, Business Associate shall take:

- a. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
  - b. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
2. **Investigation and Investigation Report.** To immediately investigate such security incident, breach, or unauthorized access, use or disclosure of PHI or PI. Within 72 hours of the discovery, Business Associate shall submit an updated "CDPH Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Information Security Officer:
  3. **Complete Report.** To provide a complete report of the investigation to the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "CDPH Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, the HIPAA regulations and/or state law. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If CDPH requests information in addition to that listed on the "CDPH Privacy Incident Report" form, Business Associate shall make reasonable efforts to provide CDPH with such information. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "CDPH Privacy Incident Report" form. CDPH will review and approve the determination of whether a breach occurred and individual notifications are required, and the corrective action plan.
  4. **Notification of Individuals.** If the cause of a breach of PHI or PI is attributable to Business Associate or its subcontractors, agents or vendors, Business Associate shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The notifications shall comply with the requirements set forth in 42 U.S.C. section 17932 and its implementing regulations, including, but not limited to, the requirement that the notifications be

Exhibit D  
HIPAA Business Associate Addendum

made without unreasonable delay and in no event later than 60 calendar days. The CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Information Security Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made.

5. **Responsibility for Reporting of Breaches.** If the cause of a breach of PHI or PI is attributable to Business Associate or its agents, subcontractors or vendors, Business Associate is responsible for all required reporting of the breach as specified in 42 U.S.C. section 17932 and its implementing regulations, including notification to media outlets and to the Secretary. If a breach of unsecured PHI involves more than 500 residents of the State of California or its jurisdiction, Business Associate shall notify the Secretary of the breach immediately upon discovery of the breach. If Business Associate has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to CDPH in addition to Business Associate, Business Associate shall notify CDPH, and CDPH and Business Associate may take appropriate action to prevent duplicate reporting. The breach reporting requirements of this paragraph are in addition to the reporting requirements set forth in subsection 1, above.
6. **CDPH Contact Information.** To direct communications to the above referenced CDPH staff, the Contractor shall initiate contact as indicated herein. CDPH reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Addendum or the Agreement to which it is incorporated.

<b>CDPH Program Contract Manager</b>	<b>CDPH Privacy Officer</b>	<b>CDPH Information Security Officer</b>
See the Scope of Work exhibit for Program Contract Manager information	Privacy Officer Privacy Office, c/o Office of Legal Services California Department of Public Health 1415 L Street, 5 <sup>th</sup> Floor Sacramento, CA 95814  Email: <a href="mailto:privacy@cdph.ca.gov">privacy@cdph.ca.gov</a> Telephone: (877) 421-9634	Chief Information Security Officer Information Security Office California Department of Public Health P.O. Box 997413, MS 6302 Sacramento, CA 95899-7413  Email: <a href="mailto:cdphiso@cdph.ca.gov">cdphiso@cdph.ca.gov</a> Telephone: IT Service Desk (916) 440-7000 or (800) 579-0874

Exhibit D  
HIPAA Business Associate Addendum

- K. Termination of Agreement.** In accordance with Section 13404(b) of the HITECH Act and to the extent required by the HIPAA regulations, if Business Associate knows of a material breach or violation by CDPH of this Addendum, it shall take the following steps:
1. Provide an opportunity for CDPH to cure the breach or end the violation and terminate the Agreement if CDPH does not cure the breach or end the violation within the time specified by Business Associate; or
  2. Immediately terminate the Agreement if CDPH has breached a material term of the Addendum and cure is not possible.
- L. Due Diligence.** Business Associate shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Addendum and is in compliance with applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, and that its agents, subcontractors and vendors are in compliance with their obligations as required by this Addendum.
- M. Sanctions and/or Penalties.** Business Associate understands that a failure to comply with the provisions of HIPAA, the HITECH Act and the HIPAA regulations that are applicable to Business Associate may result in the imposition of sanctions and/or penalties on Business Associate under HIPAA, the HITECH Act and the HIPAA regulations.

#### IV. Obligations of CDPH

CDPH agrees to:

- A. Notice of Privacy Practices.** Provide Business Associate with the Notice of Privacy Practices that CDPH produces in accordance with 45 CFR section 164.520, as well as any changes to such notice.
- B. Permission by Individuals for Use and Disclosure of PHI.** Provide the Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect the Business Associate's permitted or required uses and disclosures.
- C. Notification of Restrictions.** Notify the Business Associate of any restriction to the use or disclosure of PHI that CDPH has agreed to in accordance with 45 CFR section 164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.
- D. Requests Conflicting with HIPAA Rules.** Not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA regulations if done by CDPH.

#### V. Audits, Inspection and Enforcement

- A.** From time to time, CDPH may inspect the facilities, systems, books and records of Business Associate to monitor compliance with the Agreement and this Addendum. Business Associate shall promptly remedy any violation of any provision of this Addendum and shall certify the same to the CDPH Privacy Officer in writing. The fact that CDPH inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems and procedures does not relieve Business Associate of its responsibility to comply with this Addendum, nor does CDPH:



Exhibit D  
HIPAA Business Associate Addendum

1. Failure to detect or
  2. Detection, but failure to notify Business Associate or require Business Associate's remediation of any unsatisfactory practices constitute acceptance of such practice or a waiver of CDPH' enforcement rights under the Agreement and this Addendum.
- B.** If Business Associate is the subject of an audit, compliance review, or complaint investigation by the Secretary or the Office of Civil Rights, U.S. Department of Health and Human Services, that is related to the performance of its obligations pursuant to this HIPAA Business Associate Addendum, Business Associate shall notify CDPH and provide CDPH with a copy of any PHI or PI that Business Associate provides to the Secretary or the Office of Civil Rights concurrently with providing such PHI or PI to the Secretary. Business Associate is responsible for any civil penalties assessed due to an audit or investigation of Business Associate, in accordance with 42 U.S.C. section 17934(c).

## VI. Termination

- A. Term.** The Term of this Addendum shall commence as of the effective date of this Addendum and shall extend beyond the termination of the Agreement and shall terminate when all the PHI provided by CDPH to Business Associate, or created or received by Business Associate on behalf of CDPH, is destroyed or returned to CDPH, in accordance with 45 CFR 164.504(e)(2)(ii)(I).
- B. Termination for Cause.** In accordance with 45 CFR section 164.504(e)(1)(ii), upon CDPH' knowledge of a material breach or violation of this Addendum by Business Associate, CDPH shall:
1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate the Agreement if Business Associate does not cure the breach or end the violation within the time specified by CDPH; or
  2. Immediately terminate the Agreement if Business Associate has breached a material term of this Addendum and cure is not possible.
- C. Judicial or Administrative Proceedings.** Business Associate will notify CDPH if it is named as a defendant in a criminal proceeding for a violation of HIPAA. CDPH may terminate the Agreement if Business Associate is found guilty of a criminal violation of HIPAA. CDPH may terminate the Agreement if a finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA, or other security or privacy laws is made in any administrative or civil proceeding in which the Business Associate is a party or has been joined.
- D. Effect of Termination.** Upon termination or expiration of the Agreement for any reason, Business Associate shall return or destroy all PHI received from CDPH (or created or received by Business Associate on behalf of CDPH) that Business Associate still maintains in any form, and shall retain no copies of such PHI. If return or destruction is not feasible, Business Associate shall notify CDPH of the conditions that make the return or destruction infeasible, and CDPH and Business Associate shall determine the terms and conditions under which Business Associate may retain the PHI. Business Associate shall continue to extend the protections of this Addendum to such PHI, and shall limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate.

## VII. Miscellaneous Provisions

- A. Disclaimer.** CDPH makes no warranty or representation that compliance by Business Associate with this Addendum, HIPAA or the HIPAA regulations will be adequate or satisfactory for Business

Exhibit D  
HIPAA Business Associate Addendum

Associate's own purposes or that any information in Business Associate's possession or control, or transmitted or received by Business Associate, is or will be secure from unauthorized use or disclosure. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.

- B. Amendment.** The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Addendum may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations and other applicable laws relating to the security or privacy of PHI. Upon CDPH' request, Business Associate agrees to promptly enter into negotiations with CDPH concerning an amendment to this Addendum embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations or other applicable laws. CDPH may terminate the Agreement upon thirty (30) days written notice in the event:
1. Business Associate does not promptly enter into negotiations to amend this Addendum when requested by CDPH pursuant to this Section; or
  2. Business Associate does not enter into an amendment providing assurances regarding the safeguarding of PHI that CDPH in its sole discretion, deems sufficient to satisfy the standards and requirements of HIPAA and the HIPAA regulations.
- C. Assistance in Litigation or Administrative Proceedings.** Business Associate shall make itself and any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under the Agreement, available to CDPH at no cost to CDPH to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CDPH, its directors, officers or employees based upon claimed violation of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inactions or actions by the Business Associate, except where Business Associate or its subcontractor, employee or agent is a named adverse party.
- D. No Third-Party Beneficiaries.** Nothing express or implied in the terms and conditions of this Addendum is intended to confer, nor shall anything herein confer, upon any person other than CDPH or Business Associate and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.
- E. Interpretation.** The terms and conditions in this Addendum shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the HIPAA regulations and applicable state laws. The parties agree that any ambiguity in the terms and conditions of this Addendum shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act and the HIPAA regulations.
- F. Regulatory References.** A reference in the terms and conditions of this Addendum to a section in the HIPAA regulations means the section as in effect or as amended.
- G. Survival.** The respective rights and obligations of Business Associate under Section VI.D of this Addendum shall survive the termination or expiration of the Agreement.
- H. No Waiver of Obligations.** No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

Exhibit D  
HIPAA Business Associate Addendum

**Attachment A**  
Business Associate Data Security Requirements

**I. Personnel Controls**

- A. *Employee Training.*** All workforce members who assist in the performance of functions or activities on behalf of CDPH, or access or disclose CDPH PHI or PI must complete information privacy and security training, at least annually, at Business Associate's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following contract termination.
- B. *Employee Discipline.*** Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.
- C. *Confidentiality Statement.*** All persons that will be working with CDPH PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to CDPH PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for CDPH inspection for a period of six (6) years following contract termination.
- D. *Background Check.*** Before a member of the workforce may access CDPH PHI or PI, a thorough background check of that worker must be conducted, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

**II. Technical Security Controls**

- A. *Workstation/Laptop encryption.*** All workstations and laptops that process and/or store CDPH PHI or PI must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the CDPH Information Security Office.
- B. *Server Security.*** Servers containing unencrypted CDPH PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.
- C. *Minimum Necessary.*** Only the minimum necessary amount of CDPH PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.
- D. *Removable media devices.*** All electronic files that contain CDPH PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.

Exhibit D  
HIPAA Business Associate Addendum

- E. Antivirus software.** All workstations, laptops and other systems that process and/or store CDPH PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.
- F. Patch Management.** All workstations, laptops and other systems that process and/or store CDPH PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.
- G. User IDs and Password Controls.** All users must be issued a unique user name for accessing CDPH PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:
- Upper case letters (A-Z)
  - Lower case letters (a-z)
  - Arabic numerals (0-9)
  - Non-alphanumeric characters (punctuation symbols)
- H. Data Destruction.** When no longer needed, all CDPH PHI or PI must be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the CDPH Information Security Office.
- I. System Timeout.** The system providing access to CDPH PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.
- J. Warning Banners.** All systems providing access to CDPH PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.
- K. System Logging.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for CDPH PHI or PI, or which alters CDPH PHI or PI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If CDPH PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.
- L. Access Controls.** The system providing access to CDPH PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.

Exhibit D  
HIPAA Business Associate Addendum

- M. *Transmission encryption.*** All data transmissions of CDPH PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PHI can be encrypted. This requirement pertains to any type of PHI or PI in motion such as website access, file transfer, and E-Mail.
- N. *Intrusion Detection.*** All systems involved in accessing, holding, transporting, and protecting CDPH PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

### III. Audit Controls

- A. *System Security Review.*** All systems processing and/or storing CDPH PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.
- B. *Log Reviews.*** All systems processing and/or storing CDPH PHI or PI must have a routine procedure in place to review system logs for unauthorized access.
- C. *Change Control.*** All systems processing and/or storing CDPH PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

### IV. Business Continuity / Disaster Recovery Controls

- A. *Emergency Mode Operation Plan.*** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic CDPH PHI or PI in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under the Agreement for more than 24 hours.
- B. *Data Backup Plan.*** Contractor must have established documented procedures to backup CDPH PHI to maintain retrievable exact copies of CDPH PHI or PI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore CDPH PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of CDPH data.

### V. Paper Document Controls

- A. *Supervision of Data.*** CDPH PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. CDPH PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.
- B. *Escorting Visitors.*** Visitors to areas where CDPH PHI or PI is contained shall be escorted and CDPH PHI or PI shall be kept out of sight while visitors are in the area.
- C. *Confidential Destruction.*** CDPH PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.

Exhibit D  
HIPAA Business Associate Addendum

- D. *Removal of Data.*** CDPH PHI or PI must not be removed from the premises of the Contractor except with express written permission of CDPH.
- E. *Faxing.*** Faxes containing CDPH PHI or PI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.
- F. *Mailing.*** Mailings of CDPH PHI or PI shall be sealed and secured from damage or inappropriate viewing of PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of CDPH PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of CDPH to use another method is obtained.

**Exhibit F, A01**  
**Security Requirements, Protections, and Confidentiality Checklist**

Site Name: \_\_\_\_\_ Site Number: \_\_\_\_\_

The Contractor shall complete and return this checklist with the signed copy of the contract agreement. To complete this checklist, the authorized agency administrator or representative attests by checking the boxes adjacent to the statement and signing this checklist that the ADAP Enrollment Site meets, and shall continue to meet throughout the life of the contract (July 1, 2016 – June 30, 2020), the requirements as identified in the Scope of Work which includes those identified below:

1.	The Contractor has reviewed and attests that the contracting agency or organization meets the requirements as written in the "Nondiscrimination Clause (OCP-1)" STD 17A form and has a process in place to deal with discrimination complaints.	
2.	The Contractor can ensure the administrative, physical and technical safeguards of protected health information as required in the CDPH HIPAA BAA 6-16, HIPAA Business Associate Addendum.	
2.a.	<i>Breaches of confidential client information must be immediately reported to CDPH/OA/ADAP. In the space below, please identify the process (and individual/s) your agency or organization has in place to report breaches of ADAP clients' protected health or personal information.</i>	
3.	The ADAP Notice of Privacy Practices is posted in an area at the ADAP Enrollment Site that is accessible and visible to ADAP applicants/clients.	
4.	The Contractor has internet access and scanning and uploading capabilities to allow for the creation of electronic ADAP client files within the designated ADAP's Enrollment Benefits Management secure web-based enrollment system.	
5.	The Contractor has desktop computers with internet access available for all site personnel (shared or individual) who will be performing ADAP enrollment services.	
6.	The Contractor has fax machine/s and scanner/s used to transmit and/or received ADAP client enrollment information/documentation located in a secure area at this ADAP Enrollment Site.	

*All of the requirements listed above must be met in order to become an ADAP Enrollment Site.*

\_\_\_\_\_  
 Print Name of Authorized Agency Representative

\_\_\_\_\_  
 Title

\_\_\_\_\_  
 Signature

\_\_\_\_\_  
 Date

## Exhibit G

<b>Plan for Transporting Confidential ADAP Client Files</b>	
Enrollment Site Number:	Enrollment Site Contact:
Address of New Location (where client files are being transferred to):  Enrollment Site Name: Current Enrollment Site Address:  Enrollment Site Telephone Number:  Enrollment Site Fax Number:	Date Client Files will be Transferred:
Please submit the completed Document Transfer Plan to your CDPH ADAP Advisor.  Your advisor will contact you after the Document Transfer Plan has been reviewed/approved.	
<b>Acknowledge ADAP Policy for Transferring Client Files:</b>  It is the policy of [Insert Name of Enrollment Site], ADAP, to ensure that any transfer of ADAP documentation will be safe, secured and implemented in accordance with CDPH ADAP confidentiality and security requirements for safeguarding the confidentiality of protected health information. ADAP Eligibility Workers (EWs) will implement reasonable and appropriate administrative, technical, and physical measures to safeguard protected health information from any intentional or unintentional use or disclosure that might violate County, State or Federal privacy regulations, Health and Safety Code, and in accordance with the ADAP Site Agreement for years 2016 – 2020, Exhibit D, HIPAA Business Associate Addendum and Exhibit G, Plan for Transporting Confidential ADAP Client Files.	
<b>Why are client files being transferred?</b>  <input type="checkbox"/> Relocation of the ADAP Enrollment Site to a new office/location  <input type="checkbox"/> Providing in-home client enrollment services when a client is unable to travel to the ADAP Enrollment Site  <input type="checkbox"/> Relocating ADAP files to a new location for storage purposes  <input type="checkbox"/> Closure of an ADAP Enrollment Site.  <b>Note: If files are being transferred for a reason not listed above, please contact your ADAP Advisor</b>	
1. How many client files will be transferred?	



2. Describe the methods that will be used to secure client files when being transferred (e.g., locked container, by vehicle/trunk, no stops on way to new location, etc.)	
3. Which site staff person/s will supervise the security and transfer of client files as they are moved to the new location? Will a vendor be utilized? If so, please explain.	
4. Please describe where and how the client files will be stored at their new location.	
5. In this section, outline, step-by-step, the process that will be followed in the transferring of client files to their new location. Attach an additional page if necessary.	
_____ SIGNATURE OF SITE CONTACT/AGENCY ADMINISTRATOR	_____ DATE SIGNED

**Additional Comments:**

## **EXHIBIT 2**



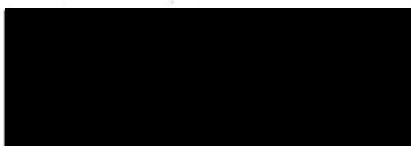
State of California—Health and Human Services Agency  
California Department of Public Health



GAVIN NEWSOM  
Governor

SONIA Y. ANGELL, MD, MPH  
State Public Health Officer & Director

June 30, 2020



**NOTICE OF DATA BREACH**

Dear 

We are writing to you because the California Department of Public Health (CDPH) experienced a privacy breach involving your personal information.

**What Happened?**

On April 30, 2020, CDPH was notified by a CDPH contractor that a former employee of the CDPH contractor had disclosed some of your personal information without authorization. Our investigation determined this disclosure happened on or around April 22, 2019.

**What Information Was Involved?**

Your full name, public health program participant information, program eligibility dates, date of birth, medical information, phone number, email, and health insurance provider name were involved.

Please note, the information did not include any other information, such as Social Security number, Driver's License number, or financial account numbers which could expose you to financial identity theft.

**What We Are Doing:**

We regret that this incident occurred. We are working to retrieve your information, ending our relationship with the contractor involved, and conducting a privacy and security audit of similar public health program contractors.

**What You Can Do:**

Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider or plan to serve as a baseline.



**Other Important Information:**

Enclosure "Breach Help –Consumer Tips from the California Attorney General"

**For More Information:**

For additional privacy protection resources, you may visit the website of the California Department of Justice, Privacy Unit at <https://www.oag.ca.gov/privacy>.

**Agency Contact:**

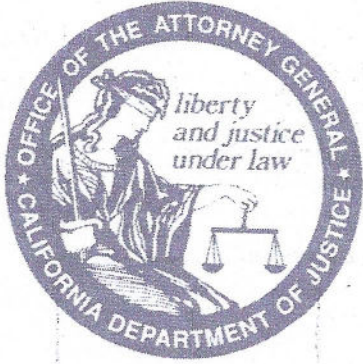
Should you need any further information about this incident, please contact the Client Services Call Center at (844) 729-4202.

Sincerely,

A handwritten signature in black ink, appearing to read "Drew Brereton". The signature is fluid and cursive, with a large initial "D" and "B".

Drew Brereton  
Deputy Director, Office of Legal Services | Chief Counsel

Enclosure



# Breach Help

## Consumer Tips from the California Attorney General

Consumer Information Sheet 17 • October 2014

You get a letter from a company, a government agency, a university, a hospital or other organization. The letter says your personal information may have been involved in a data breach. Or maybe you learn about a breach from a news report or company web site. Either way, a breach notice does not mean that you are a victim of identity theft or other harm, but you could be at risk.

The breach notice should tell you what specific types of personal information were involved. It may also tell you what the organization is doing in response. There are steps you can take to protect yourself. What to do depends on the type of personal information involved in the breach.

Note that credit monitoring, which is often offered by breached companies, alerts you *after* someone has applied for or opened new credit in your name. Credit monitoring can be helpful in the case of a Social Security number breach. It does not alert you to fraudulent activity on your existing credit or debit card account.

### **Credit or Debit Card Number**

The breach notice should tell you when and where the breach occurred. If you used your credit or debit card at the location during the given time, you can take steps to protect yourself.

### **Credit Card**

1. Monitor your credit card account for suspicious transactions and report any to the card-issuing bank (or American Express or Discover). Ask the bank for online monitoring and alerts on the card account. This will give you early warning of any fraudulent transactions.
2. Consider cancelling your credit card if you see fraudulent transactions on it following the breach. You can dispute fraudulent

transactions on your credit card statement, and deduct them from the total due. Your liability for fraudulent transactions is limited to \$50 when you report them, and most banks have a zero-liability policy.<sup>1</sup>

3. If you do cancel your credit card, remember to contact any companies to which you make automatic payments on the card. Give them your new account number if you wish to transfer the payments.

### **Debit Card**

1. Monitor your debit card account for suspicious transactions and report any to the card issuer. Ask the bank for online monitoring and alerts on the card account. This will give you early warning of any fraudulent transactions.

1. Change your password for the affected account. If you find that you are locked out of your account, contact the company's customer service or security department.
2. If you use the same password for other accounts, change them too.
3. If a security question and answer was involved, change it. Don't use questions based on information that is publicly available, such as your mother's maiden name, your pet's name or the name of your high school.
4. Use different passwords for your online accounts. This is especially important for accounts that contain sensitive information, such as your medical or financial information. Consider accounts at online merchants where you may have your credit card number stored in the account.
5. Create strong passwords. Longer is better—at least ten characters long and a mix of uppercase and lowercase letters, numerals, punctuation marks, and symbols. Don't use words found in a dictionary. You can base passwords on a phrase, song or book title.  
*Example: "I love tropical sunsets" becomes 1luvtr0p1calSuns3ts!*
6. A password manager or password "safe" can help you create and manage many strong passwords. These software programs can run on your computer, your phone and other portable devices. You only have to remember one password (or passphrase) to open the safe. The Electronic Frontier Foundation ([www.eff.org](http://www.eff.org)) lists some free versions and computer magazines offer product reviews.

### **Bank Information**

If the breach notice says your checking account number, on a check for example, was breached, here's what to do.

1. Call the bank, tell them about the breach and tell them you want to close your account. Find out what checks are outstanding. You may want to wait until they have cleared before closing the account. (Or you could write to each recipient, tell them about the breach, ask them not to process the old check and enclose a new check on your new account.)
2. Open a new bank account. Tell the bank you want to use a new password for access to your new account. Do not use your mother's maiden name or the last four digits of your Social Security number. Ask your bank to notify the check verification company it uses that the old account was closed.

### **Driver's License Number**

If the breach notice says your driver's license or California identification card number was involved, and you suspect that you are a victim of identity theft, contact DMV's Driver License Fraud and Analysis Unit (DLFAU) by telephone at 1 866-658-5758 or by email at [dlfraud@dmv.ca.gov](mailto:dlfraud@dmv.ca.gov). Do not include personal information on your e-mail.

### **Medical or Health Insurance Information**

If the breach notice says your health insurance or health plan number was involved, here's what you can do to protect yourself against possible medical identity theft. A breach that involves other medical information, but not your insurance or plan number, does not generally pose a risk of medical identity theft.

1. If the letter says your Social Security number was involved, see section on Social Security number breaches. Also contact your insurer or health plan, as in number 2 below.
2. If the letter says your health insurance or health plan number was involved, contact

your insurer or plan. Tell them about the breach and ask them to note the breach in their records and to flag your account number.

3. Closely watch the Explanation of Benefits statements for any questionable items. An Explanation of Benefits statement comes in the mail, often marked "This is not a bill." It lists the medical services received by you or anyone covered by your plan. If you see a service that you did not receive, follow

up on it with your insurer or plan. For more on medical identity theft, see *First Aid for Medical Identity Theft: Tips for Consumers*, at [www.oag.ca.gov/privacy/info-sheets](http://www.oag.ca.gov/privacy/info-sheets).

For more details on what to do if you suspect that your information is being used to commit identity theft, see the *Identity Theft Victim Checklist* at [www.oag.ca.gov/idtheft/information-sheets](http://www.oag.ca.gov/idtheft/information-sheets).

This fact sheet is for informational purposes and should not be construed as legal advice or as policy of the State of California. If you want advice on a particular case, you should consult an attorney or other expert. The fact sheet may be copied, if (1) the meaning of the copied text is not changed or misrepresented, (2) credit is given to the California Department of Justice, and (3) all copies are distributed free of charge.

#### NOTES

<sup>1</sup> Truth in Lending Act, 14 U.S. Code sec. 1601 and following.

<sup>2</sup> Electronic Funds Transfer Act, 15 U.S. Code sec. 1693 and following.



## **EXHIBIT 3**



SONIA Y. ANGELL, MD, MPH  
State Public Health Officer & Director

State of California—Health and Human Services Agency  
California Department of Public Health



GAVIN NEWSOM  
Governor

7/31/2020

Dear Jerry Flanagan,

We have received your Public Records Act request reference number P009736-072320. You have requested that CDPH provide records sufficient to establish the following:

1. Which CDPH contractor was involved in the privacy breach that happened on or around April 22, 2019?
2. What information was disclosed?
3. Who was the information disclosed to?
4. How many consumers were impacted by the privacy breach?

Enclosed you will find the Thrive Tribe Breach FAQ which will answer questions one through three listed above. Based on our investigation, we believe 460 individuals were affected by this incident. The only responsive document, upon which this number is based, is exempt from release under Government Code section 6254(c) as it contains personal medical information.

If you have any questions, please contact Edna Martin at [Edna.Martin@cdph.ca.gov](mailto:Edna.Martin@cdph.ca.gov).

Thank you,

Sandra Robinson, MBA  
ADAP Branch Chief  
California Department of Public Health



## 20-PO-DOA-39465 FAQ

### **Breach Specifics**

**1. What happened/How was my information breached?**

In late April 2020, the California Department of Public Health (CDPH) became aware that The Thrive Tribe Foundation disclosed your information to unauthorized recipients in April 2019.

**2. Who breached or accessed my personal information?**

Your information was disclosed by The Thrive Tribe Foundation to three unauthorized health-related entities, including a pharmacy benefits company, an entity trying to become an ADAP enrollment site, and a health care coordination company. We have no reason to believe your information was shared outside of these three companies.

**3. Who are the three unauthorized health-related entities?**

CDPH is working to retrieve your information. The three unauthorized healthcare entities that received your information are Adherence Project, Evolve Healthcare, and Premier Pharmacy.

**4. What sort of personal information/specific types of personal information of mine was breached?**

The disclosure included your first and last name, date of birth, contact information, ADAP identification number, and ADAP enrollment status, and eligibility end date.

**5. Where is my personal information now?**

CDPH is currently attempting to retrieve your information from the unauthorized entities. The contract with The Thrive Tribe Foundation expired on June 30, 2020 and CDPH will not be entering into a new contract with this organization.

**6. When was this breach discovered?**

CDPH has been investigating this possible breach of confidential information since April 30, 2020. On May 27, 2020, CDPH determined that a breach likely occurred.

**7. Why did you wait one year to tell me about the breach?**

CDPH was informed on April 29, 2020 of the incident that occurred in April 2019. Please note, notification to CDPH was provided more than a year after the unauthorized disclosure. Since CDPH was informed, CDPH thoroughly investigated this incident to determine what happened and whether the disclosure was a breach.

**8. What is CDPH doing about the breach? How will CDPH prevent this from happening in the future?**

CDPH let the contract with The Thrive Tribe Foundation expire on June 30, 2020, and CDPH will not be entering into a new contract with this organization. CDPH is also auditing enrollment sites to ensure they adhere to the Health Insurance Portability and Accountability Act (HIPAA) Business Associate Addendum (BAA) set forth in their contracts. The HIPAA BAA ensures that CDPH enrollment sites have adequate controls and safeguards in place to protect the privacy and security of personal information of program clients. CDPH is also making efforts to retrieve the information from the unauthorized individuals.

**9. Why wasn't my information secure?**

The incident did not occur due to a lack of security controls, but instead due to the Thrive Tribe Foundation disclosing your information to other unauthorized health care entities.

**10. What did CDPH do when it first became aware of the breach?**

Upon learning that The Thrive Tribe may have improperly disclosed client information CDPH began an investigation.

**11. I have received 2 letters from CDPH in the last couple weeks. I called the phone number in the most recent letter but it was only a voicemail. The first letter said I had to choose a new enrollment site, the second letter says my personal information was disclosed. Was it my enrollment site who disclosed my personal information?**

Yes, your previous enrollment site is the one who disclosed your personal information. As CDPH became aware of the severity of the breach and decided to let your previous enrollment site's contract expire, CDPH made efforts to ensure program clients would not experience a lapse in services and could be referred to a new enrollment site.

**12. I talked to my enrollment site, they said CDPH did not renew their contract due to budgetary concerns. Is that accurate?**

Yes. With the current budget restraints and CDPH's resource obligations in the COVID-19 response, CDPH is being asked to cut money wherever we can. Given the severity of the enrollment site's breach, CDPH spent a lot of time, money, and resources to investigate the breach, and continues to spend time, money, and resources to ensure our program clients are protected.

**Credit/Identity Theft**

**13. Does this mean that I'm a victim of identity theft?** No. The fact that someone may have had access to your information doesn't mean that your information was used to commit identity theft or that your information will be used to commit fraud. CDPH wanted to let you know about the incident so that you can take

appropriate steps to protect yourself. In addition, the information disclosed did not include any other information, such as Social Security number, Driver's License number, or financial account numbers which could expose you to financial identity theft.

**14. How will I know if any of my personal information was already used by someone else?**

You may want to request a copy of your medical records from your provider or plan to serve as a baseline and determine whether your medical records include office visits you didn't make or treatment you didn't receive.

**15. What can I do to protect myself?** You can place a fraud alert on your credit files. To place a fraud alert, call any one of the three credit bureaus at the following numbers and follow the "fraud victim" instructions. The one you call will notify the others to place the alert. When you call the credit bureau's fraud line, you will be asked for identifying information.

- **Trans Union – 1-800-680-7289**
- **Experian – 1-888-397-3742**
- **Equifax – 1-800-525-6285**

**16. What does a fraud alert do?**

A fraud alert can help protect you from identity theft. Businesses are required to verify your identity before issuing credit when you have a fraud alert and may try to contact you. A fraud alert is free, and an initial alert lasts for at least 90 days.

**17. I called the credit bureau fraud line, and they asked for my Social Security number; is it okay to give it?** Yes. The credit bureaus ask for your Social Security number and other information in order to identify you and avoid sending your credit report to the wrong person.

**18. What happens if I find out that I have been a victim of identity theft?** You can immediately notify your local law enforcement agency, contact any creditors involved, and notify the credit bureaus. For more information on what to do, see the Identity Theft Victim Checklist on the Identity Theft page of the California Office of Privacy's Web site at [www.privacy.ca.gov](http://www.privacy.ca.gov).

**19. The notice from CDPH is regarding a family member, a spouse, or child, who is deceased. What should I do?** See the Information Sheet, *Identity Theft and the Deceased* on the Identity Theft page of the California Office of Privacy's Web site at [www.privacy.ca.gov](http://www.privacy.ca.gov).

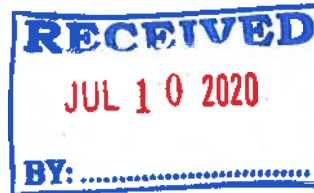
## **EXHIBIT 4**



State of California—Health and Human Services Agency  
California Department of Public Health



GAVIN NEWSOM  
Governor



July 7, 2020

Evolve Healthcare  
5670 Wilshire Blvd., Ste. 1740  
Los Angeles, CA 90036

To Whom It May Concern:

We are writing to you because the California Department of Public Health (CDPH) Privacy Office was recently informed that the following confidential CDPH information was provided to you without authorization on or around April 22, 2019:

1. The Thrive Tribe Client Log: a list of active clients of The Thrive Tribe as of April 2019, which included confidential information about the clients.

As you are not an authorized recipient of this information, please immediately destroy the confidential CDPH information, which CDPH has reason to believe is still in your possession. Please fill out the enclosed documents certifying destruction and whether any further unauthorized disclosure took place and return to [privacy@cdph.ca.gov](mailto:privacy@cdph.ca.gov) by **close of business on July 16, 2020.**

Sincerely,

Privacy Office  
California Department of Public Health

Attachments



## Instructions for Completion of Destruction and Non-Disclosure Forms

In order to document that the data files described below, which were received by you have not been disclosed to any unauthorized person and have been confidentially destroyed, we request that you complete the steps set out below.

### Any and all records or information related to: The Thrive Tribe Client Log received on or around April 22, 2019

#### **Part 1 – Deletion of electronic file(s)**

The file(s) need to be removed in the following manner:

A secure wipe (overwrite) in accordance with Department of Defense (DoD) Media Sanitization Standards should be performed. Perform either a secure erase of the individual files or a secure wipe of the free space if a normal delete has already been completed.

The Attestation of Destruction form should be completed once these practices have been completed.

#### **Part 2 – Deletion of paper file(s)**

All paper files should be destroyed by pulverizing them or using a confidential shred method.

#### **Part 3 – Non-Disclosure by Individuals**

Any individual who would have come into contact with these files will need to complete the Attestation of Non-Disclosure form. Please supply these forms to us for each person who may have come in contact with the data.

Thank you for your cooperation with these instructions.



Attestation of Destruction Form

I, \_\_\_\_\_, hereby attest the data files described below, which were received by me have been confidentially destroyed:

**Any and all records or information related to The Thrive Tribe Client Log received on or around April 22, 2019**

The Electronic records were destroyed on \_\_\_\_\_ by performing a secure erase of the individual files listed below, or a secure wipe of the free space if a normal delete has already been completed.

The Paper files were destroyed on \_\_\_\_\_ by pulverizing them or using a confidential shred method.

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Date)

Attestation of Non-Disclosure Form

I, \_\_\_\_\_, hereby attest that in relation to the information listed below,

**Any and all records or information related to The Thrive Tribe Client List received on or around April 22, 2019**

I have not disclosed the data files listed above to anyone.

I have disclosed the data files listed above to the following persons:

1. \_\_\_\_\_

2. \_\_\_\_\_

3. \_\_\_\_\_

I will not further disclose any information related to the individual(s) listed above.

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Date)

## **EXHIBIT 5**

**Agreement by Employee/Contractor to Comply with Confidentiality Requirements**

*Summary of Statutes Pertaining to Confidential Public Health Records and Penalties for Disclosure*

All HIV/AIDS case reports and any information collected or maintained in the course of surveillance-related activities that may directly or indirectly identify an individual are considered *confidential public health record(s)* under California Health and Safety Code (HSC), Section 121035(c) and must be handled with the utmost confidentiality. Furthermore, HSC §121025(a) prohibits the disclosure of HIV/AIDS-related public health records that contain any personally identifying information to any third party, unless authorized by law for public health purposes, or by the written consent of the individual identified in the record or his/her guardian/conservator. Except as permitted by law, any person who negligently discloses information contained in a confidential public health record to a third party is subject to a civil penalty of up to \$5,000 plus court costs, as provided in HSC §121025(e)(1). Any person who willfully or maliciously discloses the content of a public health record, except as authorized by law, is subject to a civil penalty of \$5,000-\$25,000 plus court costs as provided by HSC §121025(e)(2). Any willful, malicious, or negligent disclosure of information contained in a public health record in violation of state law that results in economic, bodily, or psychological harm to the person named in the record is a misdemeanor, punishable by imprisonment for a period of up to one year and/or a fine of up to \$25,000 plus court costs (HSC §121025(e)(3)). Any person who is guilty of a confidentiality infringement of the foregoing type may be sued by the injured party and shall be personally liable for all actual damages incurred for economic, bodily, or psychological harm as a result of the breach (HSC §121025(e)(4)). Each disclosure in violation of California law is a separate, actionable offense (HSC §121025(e)(5)).

Because an assurance of case confidentiality is the foremost concern of the California Department of Public Health, Office of AIDS (CDPH/OA), any actual or potential breach of confidentiality shall be immediately reported. In the event of any suspected breach, staff shall immediately notify the director or supervisor of the local health department’s HIV/AIDS surveillance unit who in turn shall notify the CDPH/OA Surveillance Section Chief or designee. CDPH/OA, in conjunction with the local health department and the local health officer shall promptly investigate the suspected breach. Any evidence of an actual breach shall be reported to the law enforcement agency that has jurisdiction.

*Employee Confidentiality Pledge*

I recognize that in carrying out my assigned duties, I may obtain access to private information about persons diagnosed with HIV or AIDS that was provided under an assurance of confidentiality. I understand that I am prohibited from disclosing or otherwise releasing any personally identifying information, either directly or indirectly, about any individual named in any HIV/AIDS confidential public health record. Should I be responsible for any breach of confidentiality, I understand that civil and/or criminal penalties may be brought against me. I acknowledge that my responsibility to ensure the privacy of protected health information contained in any electronic records, paper documents, or verbal communications to which I may gain access shall not expire, even after my employment or affiliation with the Department has terminated.

By my signature, I acknowledge that I have read, understand, and agree to comply with the terms and conditions above.

\_\_\_\_\_  
Employee name (print)

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Supervisor name (print)

\_\_\_\_\_  
Supervisor Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Name of Employer

**PLEASE RETAIN A COPY OF THIS DOCUMENT FOR YOUR RECORDS.**