RESOLUTION AGREEMENT

I. Recitals

1. Parties. The Parties to this Resolution Agreement ("Agreement") are:

A. The United States Department of Health and Human Services, Office for Civil Rights ("HHS"), which enforces the Federal standards that govern the privacy of individually identifiable health information (45 C.F.R. Part 160 and Subparts A and E of Part 164, the "Privacy Rule"), the Federal standards that govern the security of electronic individually identifiable health information (45 C.F.R. Part 160 and Subparts A and C of Part 164, the "Security Rule"), and the Federal standards for notification in the case of breach of unsecured protected health information (45 C.F.R. Part 160 and Subparts A and D of 45 C.F.R. Part 164, the "Breach Notification Rule"). HHS has the authority to conduct compliance reviews and investigations of complaints alleging violations of the Privacy, Security, and Breach Notification Rules (the "HIPAA Rules") by covered entities and business associates, and covered entities and business associates must cooperate with HHS compliance reviews and investigations. *See* 45 C.F.R. §§ 160.306(c), 160.308, and 160.310(b).

B. PIH Health, Inc. ("PIH"), which meets the definition of a Covered Entity as defined at 45 C.F.R. § 160.103, and therefore is required to comply with the HIPAA Rules.

C. HHS and PIH shall together be referred to herein as the "Parties."

2. Factual Background and Covered Conduct.

HHS initiated an investigation of PIH on April 29, 2020, pursuant to a breach report submitted by PIH to OCR on January 10, 2020. OCR's investigation revealed that PHI's breach occurred between June 11 and June 21, 2019, where 45 employee email accounts were compromised by a targeted phishing attack that exposed the electronic protected health information (ePHI) of 189,763 individuals.
HHS's investigation of the incident indicated potential violations of the following provisions ("Covered Conduct"):

A. The requirement to not use or disclose PHI except as permitted by the Privacy Rule (see 45 C.F.R. § 164.502(a)).
B. The requirement to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI held by PIH (see 45 C.F.R. § 164.308(a)(1)(ii)(A)).
C. The requirement to notify affected individuals of a breach within 60 days of discovery of the breach (see 45 C.F.R. § 164.404(a)).
D. The requirement to notify the media of a breach of over 500 individuals within 60 days of discovery of the breach (see 45 C.F.R. § 164.406).
E. The requirement to notify the HHS Secretary of a breach within 60 days of discovery of the breach (see 45 C.F.R. § 164.408).

3. No Admission. This Agreement is not an admission of liability by PIH.

4. No Concession. This Agreement is not a concession by HHS that PIH is not in violation of the HIPAA Rules and not liable for civil money penalties ("CMPs").

5. Intention of Parties to Effect Resolution. This Agreement is intended to resolve OCR Transaction Number: 20-370297 and any potential violations of the HIPAA Rules related to the Covered Conduct associated with the compliance review and investigation specified in paragraph I.2 of this Agreement. In consideration of the Parties' interest in avoiding the uncertainty, burden, and expense of further investigation and formal proceedings, the Parties agree to resolve this matter according to the Terms and Conditions below.

II. Terms and Conditions

6. Payment. HHS has agreed to accept, and PIH has agreed to pay HHS, the amount of **$600,000** ("Resolution Amount"). PIH agrees to pay the Resolution Amount in one lump sum within fifteen (15) days of the Effective Date of this Agreement as defined in paragraph II.14 pursuant to written instructions to be provided by HHS.

7. Corrective Action Plan. PIH has entered into and agrees to comply with the Corrective Action Plan ("CAP"), attached as Appendix B, which is incorporated into this Agreement by reference. If PIH breaches the CAP and fails to cure the breach as set forth in the CAP, then PIH will be in breach of this Agreement and HHS will not be subject to the Release set forth in paragraph II.8 of this Agreement.

8. Release by HHS. In consideration of and conditioned upon PIH's performance of its obligations under this Agreement, HHS releases PIH from any actions it may have against PIH under the HIPAA Rules arising out of or related to the Covered Conduct associated with the compliance review identified in paragraph I.2 of this Agreement. HHS does not release PIH from, nor waive any rights, obligations, or causes of action other than those arising out of or related to the Covered Conduct associated with the compliance review and referred to in this paragraph. This release does not extend to actions that may be brought under section 1177 of the Social Security Act, 42 U.S.C. § 1320d-6.

9. Agreement by Released Parties. PIH shall not contest the validity of its obligation to pay, nor the amount of, the Resolution Amount or any other obligations agreed to under this Agreement. PIH waives all procedural rights granted under Section 1128A of the Social Security Act (42 U.S.C. § 1320a- 7a) and 45 C.F.R. Part 160 Subpart E, and HHS claims collection regulations at 45 C.F.R. Part 30, including, but not limited to, notice, hearing, and appeal with respect to the Resolution Amount.

10. Binding on Successors. This Agreement is binding on PIH and its successors, heirs, transferees, and assigns.

11. Costs. Each Party to this Agreement shall bear its own legal and other costs incurred in connection with this matter, including the preparation and performance of this Agreement.

12. No Additional Releases. This Agreement is intended to be for the benefit of the Parties only, and by this instrument, the Parties do not release any claims against or by any other person or entity.

13. Effect of Agreement. This Agreement constitutes the complete agreement between the Parties. All material representations, understandings, and promises of the Parties are contained in this Agreement. Any modifications to this Agreement shall be set forth in writing and signed by all Parties.

14. Execution of Agreement and Effective Date. The Agreement shall become effective (*i.e.*, final and binding) upon the date of signing of this Agreement and the CAP by the last signatory ("Effective Date").

15. Tolling of Statute of Limitations. Pursuant to 42 U.S.C. § 1320a-7a(c)(1), a CMP must be imposed within six (6) years from the date of the occurrence of the violation. To ensure that this six-year period does not expire during the term of this Agreement, PIH agrees that the time between the Effective Date of this Agreement (as set forth in Paragraph 14) and the date the Agreement may be terminated by reason of PIH's breach, plus one-year thereafter, will not be included in calculating the six (6) year statute of limitations applicable to the violations which are the subject of this Agreement. PIH waives and will not plead any statute of limitations, laches, or similar defenses to any administrative action relating to the Covered Conduct associated with the compliance review identified in paragraph I.2 that is filed by HHS within the time period set forth above, except to the extent that such defenses would have been available had an administrative action been filed on the Effective Date of this Agreement.

16. Disclosure. HHS places no restriction on the publication of the Agreement. In addition, HHS may be required to disclose material related to this Agreement to any person upon request consistent with the applicable provisions of the Freedom of Information Act, 5 U.S.C. § 552, and its implementing regulations, 45 C.F.R. Part 5.

17. Execution in Counterparts. This Agreement may be executed in counterparts, each of which constitutes an original, and all of which shall constitute one and the same agreement.

18. Authorizations. The individual(s) signing this Agreement on behalf of PIH represent and warrant that they are authorized by PIH to execute this Agreement. The individual(s) signing this Agreement on behalf of HHS represent and warrant that they are signing this Agreement in their official capacities and that they are authorized to execute this Agreement.

For PIH Health, Inc.

/s/ 01/28/2025

James R. West Date
President and Chief Executive Officer
PIH Health, Inc.

For the United States Department of Health and Human Services

/s/ 01/28/2025

Michael Leoz Date
Regional Manager
Office for Civil Rights, Pacific Region

Appendix A

CORRECTIVE ACTION PLAN

BETWEEN THE

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

AND

PIH HEALTH, INC.

I. Preamble

PIH Health, Inc. (PIH) hereby enters into this Corrective Action Plan ("CAP") with the United States Department of Health and Human Services, Office for Civil Rights ("HHS"). Contemporaneously with this CAP, PIH is entering into a Resolution Agreement ("Agreement") with HHS, and this CAP is incorporated by reference into the Resolution Agreement as Appendix B. PIH enters into this CAP as part of consideration for the release set forth in paragraph II.8 of the Agreement.

II. Contact Persons and Submissions

A. Contact Persons

PIH contact persons for PIH regarding the implementation of this CAP and for receipt and submission of notifications and reports:

Anup Patel
Vice President, Enterprise Risk Management and Corporate Compliance
PIH Health, Inc.
12401 Washington Blvd.
Whittier, CA 90602

HHS has identified the following individual as its authorized representative and contact person with whom PIH is to report information regarding the implementation of this CAP:

Lesley Morgan, Investigator
Department of Health and Human Services
Office for Civil Rights, Pacific Region
90 7th Street, Suite 4-100
San Francisco, CA 94103

PIH and HHS agree to promptly notify each other of any changes in the contact persons or the other information provided above.

B. Proof of Submissions. Unless otherwise specified, all notifications and reports required by this CAP may be made by any means, including certified mail, overnight mail, or hand delivery, provided that there is proof that such notification was received. For purposes of this requirement, internal facsimile confirmation sheets do not constitute proof of receipt.

III. Effective Date and Term of CAP

The Effective Date for this CAP shall be calculated in accordance with paragraph II.14 of the Agreement ("Effective Date"). The period for compliance ("Compliance Term") with the obligations assumed by PIH under this CAP shall begin on the Effective Date of this CAP and end two (2) years from the Effective Date, unless HHS has notified PIH under section VIII hereof of its determination that PIH breached this CAP. In the event HHS notifies PIH of a breach under section VIII hereof, the Compliance Term shall not end until HHS notifies PIH that HHS has determined PIH failed to meet the requirements of section VIII.C of this CAP and issues a written notice of intent to proceed with an imposition of a civil money penalty against PIH pursuant to 45 C.F.R. Part 160. After the Compliance Term ends, PIH shall still be obligated to: (a) submit the final Annual Report as required by section VI; and (b) comply with the document retention requirement in section VII. Nothing in this CAP is intended to eliminate or modify PIH's obligation to comply with the document retention requirements in 45 C.F.R. § 164.316(b) and § 164.530(j).

IV. Time

In computing any period of time prescribed or allowed by this CAP, all days referred to shall be calendar days. The day of the act, event, or default from which the designated period of time begins to run shall not be included. The last day of the period so computed shall be included, unless it is a Saturday, a Sunday, or a legal holiday, in which event the period runs until the end of the next day which is not one of the aforementioned days.

V. Corrective Action Obligations

PIH agrees to the following:

A. Conduct an Accurate and Thorough Risk Analysis

1. PIH shall conduct and complete an accurate, thorough, enterprise-wide analysis of security risks and vulnerabilities that incorporates all electronic equipment, data systems, programs, and applications controlled, administered, owned, or shared by PIH or its affiliates that are owned, controlled or managed by PIH that contain, store, transmit, or receive PIH ePHI. As part of this process, PIH shall develop a complete inventory of all electronic equipment, data systems, off-site data storage facilities, and applications that contain or store ePHI, which will then be incorporated in its Risk Analysis.

2. Within 30 days of the Effective Date, PIH shall submit to HHS the scope and methodology by which it proposes to conduct the Risk Analysis. HHS shall notify PIH whether the proposed scope and methodology is or is not consistent with 45 C.F.R. § 164.308 (a)(l)(ii)(A). PIH shall provide the Risk Analysis, consistent with paragraph V.A.l., to HHS within 120 days of HHS's approval of the scope and methodology described in paragraph V.A.2 for HHS's review.

3. Upon submission by PIH, HHS shall review and recommend changes to the aforementioned risk analysis within 60 days. If HHS requires revisions to the Risk Analysis, HHS shall provide PIH with a detailed, written explanation of such required revisions and with comments and recommendations in order for PIH to be able to prepare a revised Risk Analysis. Upon receiving HHS's recommended changes, PIH shall have thirty (30) calendar days to submit a revised risk analysis. This process will continue until HHS provides final approval of the risk analysis.

4. PIH shall annually conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by PIH, affiliates that are owned, controlled, or managed by PIH; and document the security measures PIH implemented or is implementing to sufficiently reduce the identified risks and vulnerabilities to a reasonable and appropriate level. Subsequent risk analyses and corresponding risk management plans shall be submitted for review by HHS in the same manner as described in this section until the conclusion of the CAP. Revisions to policies and procedures in this section shall be made pursuant to section V.C.3 below.

B. Develop and Implement a Risk Management Plan

1. PIH shall develop an enterprise-wide Risk Management Plan to address and mitigate any security risks and vulnerabilities identified in the Risk Analysis specified in section V.A.1. above. The Risk Management Plan shall include a process and timeline for PIH's implementation, evaluation, and revision of its risk remediation activities.

2. Within Sixty (60) days of HHS's final approval of the Risk Analysis described in section V.A.1 above, PIH shall submit a Risk Management Plan to HHS for HHS's review and approval. HHS shall approve, or, if necessary, require revisions to PIH's Risk Management Plan.

3. Upon receiving HHS's notice of required revisions, if any, PIH shall have sixty (60) days to revise the Risk Management Plan accordingly and forward for review and approval. This process shall continue until HHS approves the Risk Management Plan.

4. Within sixty (60) days of HHS's approval of the Risk Management Plan, PIH shall finalize and officially adopt the Risk Management Plan in accordance with its applicable administrative procedures.

C. Policies and Procedures

1. PIH shall develop, maintain, and revise, as necessary, its written policies and procedures to comply with the Federal standards that govern the privacy and security of individually identifiable health information (45 C.F.R. Part 160 and Subparts A, C, and E of Part 164, the "Privacy Rule" and "Security Rule"). PIH's policies and procedures shall include, but not be limited to, the minimum content set forth in section V.E.

2. PIH shall provide such policies and procedures to HHS within (60) days of receipt of HHS's approval of the Risk Management Plan required by paragraph V.B. above. HHS shall approve, or, if necessary, require revisions to policies and procedures.

3. Upon receiving HHS's notice of required revisions, if any, PIH shall have sixty (60) days to revise the policies and procedures accordingly and provide the revised policies and procedures to HHS for review and approval. This process shall continue until HHS approves the policies and procedures.

4. Within thirty (30) days of HHS's approval of the policies and procedures, PIH shall implement such policies and procedures.

D. Distribution of Policies and Procedures

1. PIH shall distribute the policies and procedures identified in section V.C. to all members of the workforce who have access to PHI within thirty (30) days of HHS's approval of such policies and to new workforce members within thirty (30) days of their beginning of service.

2. PIH shall require, at the time of distribution of such policies and procedures, a signed written or electronic initial compliance certification from all workforce members stating that such workforce members have read, understand, and shall abide by such policies and procedures.

3. PIH shall not provide access to PHI to any workforce member if that workforce member has not signed or provided the written or electronic certification required by paragraph 2 of this section.

E. Minimum Content of the Policies and Procedures

The Policies and Procedures shall address prohibited uses of PHI in email accounts and include measures to address the following Privacy, Security, and Breach Notification Rule Provisions:

1. Impermissible Uses/Disclosures 45 C.F.R. § 164.502;
2. Risk Analysis 45 C.F.R. § 164.308(a)(1)(ii)(A);
3. Risk Management 45 C.F.R. § 164.308(a)(1)(ii)(B);
4. Sanctions 45 C.F.R. § 164.308(a)(1)(ii)(C);
5. Information System Activity Review 45 C.F.R. § 164.308(a)(1)(ii)(D);
6. Security Awareness and Training 45 C.F.R. § 164.308(a)(5)(i);
7. Breach Notification 45 C.F.R. §§ 164.404(a), 164.406, and 164.408.

F. Training

1. Within thirty (30) days of HHS's final approval of the policies and procedures required by section V.C. of this CAP, PIH shall augment its existing HIPAA and Security Training Program ("Training Program") for all PIH workforce members who have access to PHI. The Training Program shall include general instruction on compliance with PIH's HIPAA policies and procedures. PIH shall submit its proposed training materials on the policies and procedures to HHS for its review and approval. HHS shall approve, or, if necessary, require revisions to PIH's Training Program.

2. Upon receiving HHS's notice of required revisions, if any, PIH shall have sixty (60) days to revise the Training Program accordingly and forward to HHS for review and approval. This process shall continue until HHS approves the Training Program.

3. Within sixty (60) days after receiving HHS's final approval of the Training Program and at least every 12 months thereafter, PIH shall provide training to all appropriate workforce members who have access to PHI within thirty (30) days of their beginning of service and in accordance with PIH's applicable administrative procedures for training.

4. Notwithstanding PIH's obligation to train its workforce members on revised policies and procedures in section V.D. above, after providing the training required by section V.F.3, PIH shall provide annual retraining on PIH's HIPAA policies and procedures to all appropriate workforce members for the duration of the Compliance Term of this CAP.

5. Each workforce member who is required to attend training shall certify, in electronic or written form, that he or she has received the training. The training certification shall specify the date training was received. All training materials shall be retained in compliance with section VII of this CAP.

G. Reportable Events

1. During the Compliance Term, PIH shall, upon learning that a workforce member failed to comply with its HIPAA policies and procedures or the Privacy, Security or Breach Notification Rules (HIPAA Rules), promptly investigate the matter. If PIH determines, after review and investigation, that a workforce member has failed to comply with its policies and procedures or the HIPAA Rules, PIH shall immediately report the event to HHS. Such violations shall be known as Reportable Events. The report to HHS shall include the following:

a. A complete description of the event, including the relevant facts, the persons involved, and the applicable provision(s) of PIH's Privacy, Security and Breach Notification policies and procedures implicated; and

b. A description of the actions taken and any further steps PIH plans to take to address the matter to mitigate any harm, and to prevent it from recurring, including application of any appropriate sanctions against workforce members who failed to comply with its HIPAA policies and procedures or the HIPAA Rules.

2. If no Reportable Events occur during the Compliance term, PIH shall so inform HHS in the Annual Report as specified in section VI below.

VI. Implementation Report and Annual Reports

A. Implementation Report. Within one hundred and twenty (120) days after receiving HHS's approval of the Risk Management Plan, policies and procedures, and training materials consistent with section V above, PIH shall submit a written report with the documentation described below to HHS summarizing the status of its implementation of this CAP for review and approval. The report, known as the "Implementation Report" shall include:

1. An attestation signed by an owner or officer of PIH attesting that the policies and procedures required by section V of this CAP: (a) have been adopted; (b) are being implemented; and (c) have been distributed to all appropriate workforce members;

2. A copy of all training materials used for the training required by this CAP, a description of the training, including a summary of the topics covered, the length of the session(s) and a schedule of when the training session(s) were held;

3. An attestation signed by an owner or officer of PIH attesting that all members of the workforce have completed the initial training required by this CAP and have executed the training certifications required by section V.F.5;

4. An attestation signed by an owner or officer of PIH listing all PIH locations (including mailing addresses), the corresponding name under which each location is doing business, the corresponding phone numbers and fax numbers, and attesting that each location has complied with the obligations of this CAP; and

5. An attestation signed by an owner or officer of PIH stating that he or she has reviewed the Implementation Report, has made a reasonable inquiry regarding its content, and believes that, upon such inquiry, the information is accurate and truthful.

B. Annual Reports. The one (1) year period beginning on the Effective Date and each subsequent one (1) year period during the course of the period of compliance obligations shall be referred to as "the Reporting Periods." PIH also shall submit to HHS Annual Reports with respect to the status of and findings regarding PIH's compliance with this CAP for each of the three Reporting Periods. PIH shall submit each Annual Report to HHS no later than sixty (60) days after the end of each corresponding Reporting Period. The Annual Report shall include:

1. A schedule, topic outline, and copies of the training materials for the training programs attended in accordance with this CAP during the Reporting Period that is the subject of the report;

2. An attestation signed by an owner or officer of PIH attesting that it is obtaining and maintaining written training certifications from all persons that require training that they received training pursuant to the requirements set forth in this CAP;

3. A summary of the annual review of PIH's Risk Analysis, as required by section V.A.4. above, and revisions, if any, to PIH's Risk Management Plan, Policies and Procedures, training materials, and implemented security measures as required by V.A.4 above.

4. A summary/description of all engagements between PIH, including, but not limited to, any outside financial audits, compliance program engagements, or reimbursement consulting, if different from what was submitted as part of the Implementation Report;

5. A summary of Reportable Events (defined in section V.G.1) identified during the Reporting Period and the status of any corrective and preventative action relating to all such Reportable Events;

6. An attestation signed by an owner or officer of PIH attesting that he or she has reviewed the Annual Report, has made a reasonable inquiry regarding its content and believes that, upon such inquiry, the information is accurate and truthful.

VII. Document Retention

PIH shall maintain for inspection and copying, and shall provide to HHS upon request, all documents and records relating to compliance with this CAP for six (6) years from the Effective Date.

VIII. Breach Provisions

PIH is expected to fully and timely comply with all provisions contained in this CAP.

A. Timely Written Requests for Extensions

PIH may, in advance of any due date set forth in this CAP, submit a timely written request for an extension of time to perform any act required by this CAP. A "timely written request" is defined as a request in writing received by HHS at least five days prior to the date such an act is required or due to be performed. This requirement may be waived by OCR only.

B. Notice of Breach of this CAP and Intent to Impose Civil Monetary Penalty. The parties agree that a breach of this CAP by PIH constitutes a breach of the Agreement. Upon a determination by HHS that PIH has breached this CAP, HHS may notify PIH of: (1) PIH's breach; and (2) HHS's intent to impose a CMP pursuant to 45 C.F.R. Part 160, or other remedies for the Covered Conduct associated with the compliance review set forth in paragraph I.2 of the Agreement and any other conduct that constitutes a violation of the HIPAA Privacy, Security, or Breach Notification Rules ("Notice of Breach and Intent to Impose CMP").

C. PIH's Response. PIH shall have thirty (30) days from the date of receipt of the Notice of Breach and Intent to Impose CMP to demonstrate to HHS's satisfaction that:

1. PIH complies with the obligations of the CAP that HHS cited as the basis for the breach;

2. The alleged breach has been cured; or

3. The alleged breach cannot be cured within the thirty (30) day period, but that: (a) PIH has begun to take action to cure the breach; (b) PIH is pursuing such action with due diligence; and (c) PIH has provided to HHS a reasonable timetable for curing the breach.

D. Imposition of CMP. If at the conclusion of the thirty (30) day period, PIH fails to meet the requirements of section VIII.C. of this CAP to HHS's satisfaction, HHS may proceed with the imposition of a CMP against PIH pursuant to 45 C.F.R. Part 160 for any violations of the Covered Conduct associated with the compliance review set forth in paragraph I.2 of the Agreement and for any other act or failure to act that constitutes a violation of the HIPAA Rules. HHS shall notify PIH in writing of its determination to proceed with the imposition of a CMP pursuant to 45 C.F.R. Part 160.

For PIH Health, Inc.

/s/ 01/28/2025

James R. West
President and Chief Executive Officer
PIH Health, Inc

Date

For United States Department of Health and Human Services

/s/ 01/28/2025

Michael Leoz
Regional Manager
Office for Civil Rights, Pacific Region

Date