

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. Lifespan ACE (“Lifespan”), which is a covered entity as defined at 45 C.F.R. §§ 160.103 and 164.105(b)(1), and therefore is required to comply with the HIPAA Rules. Lifespan is a not-for-profit health system based in Providence, R.I. Lifespan includes three academic teaching hospitals: Rhode Island Hospital and its Hasbro Children’s Hospital; The Miriam Hospital; and Bradley Hospital. It also includes Newport Hospital and Gateway Healthcare.

HHS and Lifespan shall together be referred to herein as the “Parties.”

2. Factual Background and Covered Conduct.

On Saturday, February 25, 2017, a Rhode Island Hospital employee’s car was broken into while it was parked in a public lot. One of the items stolen was a MacBook laptop used by the employee for work purposes. The laptop was never recovered. Lifespan ascertained that the employee’s work emails may have been cached in a file on the device’s hard drive. The analysis revealed that the thieves had access to: patient names, medical record numbers, demographic information, including partial address information, and the name of one or more medications that were prescribed or administered to patients. The protected health information on the stolen laptop may have included information for patients across various affiliated provider facilities and belongs to Rhode Island Hospital, Lifespan Pharmacy LLC, retail pharmacies and affiliated hospitals of Lifespan.

HHS’ investigation indicated the following covered conduct occurred (“Covered Conduct”):

- A. Lifespan did not implement policies and procedures to encrypt all devices used for work purposes (see 45 C.F.R. § 164.312(a)(2)(iv));
 - B. Lifespan did not implement policies and procedures to track or inventory all devices that access the network or which contain ePHI (See 45 C.F.R. § 164.310(d)(1));
 - C. Lifespan did not have the proper business associate agreements in place between Lifespan Corporation and the Lifespan healthcare provider affiliates that are members of the Lifespan ACE (See 45 C.F.R. § 164.502(e)); and
 - D. Lifespan impermissibly disclosed the PHI of 20,431 individuals (see 45 C.F.R. § 164.502(a)).
3. No Admission. This Agreement is not an admission of liability by Lifespan.
4. No Concession. This Agreement is not a concession by HHS that Lifespan 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 HHS Transaction Number: 01-17-268382 and any violations of the HIPAA Rules related to the Covered Conduct 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 Lifespan has agreed to pay HHS, the amount of \$1,040,000 (“Resolution Amount”). Lifespan agrees to pay the Resolution Amount on 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. Lifespan has entered into and agrees to comply with the Corrective Action Plan (“CAP”), attached as Appendix A, which is incorporated into this Agreement by reference. If Lifespan breaches the CAP, and fails to cure the breach as set forth in the CAP, then Lifespan 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 Lifespan’s performance of its obligations under this Agreement, HHS releases Lifespan from any actions it may have against Lifespan under the HIPAA Rules arising out of or related to the Covered Conduct identified in paragraph I of this Agreement. HHS does not release Lifespan from, nor waive any rights, obligations, or causes of action other than those arising out of or related to the Covered Conduct 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. Lifespan 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. Lifespan 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 Lifespan 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, Lifespan 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 Lifespan'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. Lifespan waives and will not plead any statute of limitations, laches, or similar defenses to any administrative action relating to the covered conduct 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.

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 Lifespan represent and warrant that they are authorized by Lifespan 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 Lifespan ACE



Paul J. Adler
Senior Vice President and General Counsel
Lifespan

June 26, 2020
Date

For Department of Health and Human Services



Susan M. Pezzullo Rhodes
Regional Manager
Office for Civil Rights

June 26, 2020
Date

Appendix A
CORRECTIVE ACTION PLAN
BETWEEN THE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
AND
LIFESPAN ACE

I. **Preamble**

Lifespan ACE (hereinafter known as “Lifespan”) 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, Lifespan is entering into a Resolution Agreement (“Agreement”) with HHS, and this CAP is incorporated by reference into the Resolution Agreement as Appendix A. Lifespan 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**

Lifespan has identified the following individual as its authorized representative and contact person regarding the implementation of this CAP and for receipt and for receipt and submission of notifications and reports:

Donna Schneider
Lifespan Vice President, Corporate Compliance and Internal Audit
Lifespan Compliance & Privacy Officer
225 Carolina Avenue, Suite 300
Providence, RI 02905
Office Phone: (401) 444-4728
Fax: (401) 444-5842
dschneider@lifespan.org

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

Susan M. Pezzullo Rhodes
Office for Civil Rights, New England Region
U.S. Department of Health and Human Services
JFK Federal Building, Room 1875

Boston, MA 02203
Email: Susan.Rhodes@hhs.gov
Telephone: 617-565-1347
Fax: 617-565-3809

Lifespan 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 Lifespan 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 Lifespan under section VIII hereof of its determination that Lifespan breached this CAP. After the Compliance Term ends, Lifespan 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. In the event HHS notifies Lifespan of a breach under section VIII hereof, the Compliance Term shall not end until HHS notifies Lifespan that HHS has determined Lifespan 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 Lifespan pursuant to 45 C.F.R. Part 160. Lifespan is otherwise required 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

Lifespan agrees to the following:

- A. Affiliated Covered Entity (ACE) Status

1. Within thirty (30) days of the Effective Date, Lifespan shall provide HHS with evidence of the status of the Lifespan ACE and what covered entities are members of the ACE per 45 C.F.R. § 164.105(b)(1);
2. Upon receiving any recommended changes to the ACE status from HHS, Lifespan shall have thirty (30) days to revise its ACE status accordingly and provide the revised ACE documentation to HHS for review and approval.

B. Business Associate Agreements

1. Lifespan shall revise its policies and procedures to:
 - a. Designate one or more individual(s) who are responsible for ensuring that Lifespan enters into a business associate agreement with each of its business associates, as defined by the HIPAA Rules, prior to Lifespan disclosing protected health information (PHI) to a business associate;
 - b. Create a process for assessing Lifespan's current and future business relationships to determine whether each relationship is with a "business associate," as that term is defined under the HIPAA Rules, and requires Lifespan to enter into a business associate agreement;
 - c. Create a process for negotiating and entering into business associate agreements with business associates prior to disclosing PHI to the business associates;
 - d. Create a standard template business associate agreement per 45 CFR 164.504(e);
 - e. Create a process for maintaining documentation of a business associate agreement for at least six (6) years beyond the date of when the business associate relationship is terminated; and
 - f. Limit disclosures of PHI to business associates to the minimum necessary amount of PHI that is reasonably necessary for business associates to perform their duties.
2. Lifespan shall provide the policies and procedures identified in section V.B.1 above to HHS for review and approval within sixty (60) days. Upon receiving any recommended changes to such policies and procedures from HHS, Lifespan shall have thirty (30) days to revise such policies and procedures accordingly and provide the revised policies and procedures to HHS for review and approval.

3. Within thirty (30) days of HHS' approval and annually following the Effective Date during the Compliance Term, Lifespan shall provide HHS with the following:

- a. An accounting of business associates arrangements between Lifespan Corporation and members of the Lifespan ACEs to include the names of business associates, a description of services provided, and the date services began; and
- b. Copies of the business associate agreements within the scope of V.B.3.a.

C. Encryption and Access Controls Report

1. Within ninety (90) days of the Effective Date, Lifespan shall provide proof of encryption and access controls by submitting to HHS a written report or reports regarding the status of encryption of Lifespan devices ("Encryption Report") and an update on their Network Access Controls report (NAC Report), which shall consist of:

- a. The total number of Lifespan devices and equipment including, but not limited to, desktop computers, laptop computers, tables, mobile telephones, USB drives, and medical equipment, that may be used to access, store, download, or transmit Lifespan ePHI as of the date of the Encryption Report ("Covered Electronic Media");
- b. The total number of Covered Electronic Media that are encrypted as of the date of the Encryption Report, as well as evidence of such encryption; and
- c. For any Covered Electronic Media that are not encrypted as of the date of the Encryption Report, either (i) a description of Lifespan's plan to encrypt such Covered Electronic Media and an estimate of when such Covered Electronic Media will be encrypted; or (ii) a description of why encrypting such Covered Electronic Media is not reasonable and appropriate, and a description of the compensating alternative measures implemented to safeguard the ePHI accessed, stores, downloaded, or transmitted by such Covered Electronic Media.
- d. An updated report on how Lifespan is controlling access to their network. Additionally, this NAC report should indicate what network access controls have been implemented and any pending updates to their access control policies and procedures.

2. The Covered Electronic Media included in the Encryption Report may be described and organized by category. Further, for each category of Covered Electronic Media, the Encryption Report shall document the encryption solution used (e.g., native or third party encryption product) including the version number of the encryption solution as well as the encryption algorithms/ciphers the encryption solution is configured to use. The evidence of encryption required under paragraph V.B.1.b. may be provided in the form of a screenshot that demonstrates encryption for a particular category of Covered Electronic Media, a copy of the license for the encryption software deployed on a particular category of Covered Electronic Media, or other reasonable means of demonstrating such Covered Electronic Media are encrypted.
3. Lifespan shall provide an update to HHS regarding its encryption status, which shall include:
 - a. The status, including supporting evidence, of Lifespan's implementation of a Mobile Device Management (MDM) solution that will ensure all Lifespan-owned and personally-owned mobile devices (tablets, smart phones, and other mobile devices) that access ePHI on Lifespan's secure network are encrypted, except for any mobile devices for which Lifespan has granted exceptions to the encryption requirement. If Lifespan has granted exceptions for the encryption requirement to any mobile devices, it will provide evidence of reasonable compensating controls that have been implemented to protect the ePHI on such devices. Lifespan shall complete initial deployment of an MDM solution within one hundred and twenty (120) days of the Effective Date.
 - b. Lifespan will periodically test the effectiveness of its implemented solution to enforce encryption on Lifespan-owned and personally-owned devices (laptops, desktops, and medical equipment) connecting to Lifespan's secure wired network except for any devices for which Lifespan has granted exceptions to the encryption requirement. Lifespan shall complete initial deployment of a solution to enforce encryption of ePHI on devices connecting to Lifespan's secure wireless network within one hundred and twenty (120) of the Effective Date.

D. Review and Revise Policies and Procedures

1. Lifespan shall review and revise, as necessary, Lifespan's written policies and procedures as it pertains to Device and Media Controls to comply with 45 C.F.R. § 164.310(d)(1).

2. Lifespan shall provide the policies and procedures identified in section V.D.1 above to HHS for review and approval within sixty (60) days. Upon receiving any recommended changes to such policies and procedures from HHS, Lifespan shall have thirty (30) days to revise such policies and procedures accordingly and provide the revised policies and procedures to HHS for review and approval.
3. Lifespan shall adopt (in accordance with its applicable administrative procedures) the policies and procedures approved by HHS pursuant to section V.D.2 within thirty (30) days of receipt of HHS' approval.

E. Distribution of Policies and Procedures

1. Lifespan shall distribute the policies and procedures identified in section V.D. to all members of the Lifespan's workforce who use or disclose electronically protected health information (ePHI) within thirty (30) days of HHS approval of such policies and procedures, and thereafter to new members of the workforce who will use or disclose ePHI within thirty (30) days of their becoming a member of the workforce.

F. Training

1. All Lifespan workforce members who have access to ePHI shall receive specific training on the policies and procedures submitted to HHS under section V.D. within ninety (90) days of the adoption of those policies and procedures in accordance with section V.D.3 and at least annually thereafter. Any individuals who will have access to ePHI that join Lifespan's workforce after the initial training period described in this section shall be trained within thirty (30) days of their becoming a member of the workforce.
2. Each Lifespan 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 course materials shall be retained in compliance with section VII.
3. Lifespan shall review the training at least annually, and, where appropriate, update the training to reflect changes in Federal law or HHS guidance, any issues discovered during audits or reviews, and any other relevant developments.

G. Reportable Events

1. During the Compliance Term, in the event that Lifespan receives information that a workforce member may have failed to comply with the policies and procedures submitted to HHS under sections V.D., Lifespan shall promptly

investigate this matter. If Lifespan determines, after such investigation, that during the Compliance Term a member of its workforce has failed to comply with the policies and procedures submitted to HHS under section V.D., Lifespan shall notify HHS in writing within sixty (60) days. Such violations shall be known as Reportable Events. The report to HHS shall include the following information:

- a. A complete description of the event, including the relevant facts, the persons involved, and the provision(s) of the policies and procedures implicated; and
 - b. A description of the actions taken and any further steps Lifespan plans to take to address the matter to mitigate any harm, and to prevent it from recurring, including application of appropriate sanctions against workforce members who failed to comply with the policies and procedures submitted to HHS under section V.D.
2. If no Reportable Events occur within the Compliance Term, Lifespan shall so inform HHS in its Implementation Report as specified in section VI below.

VI. **Implementation Report**

- A. Within one-hundred and eighty (180) days after HHS approves Policies and Procedures specified in section V.C. above, Lifespan shall submit a written report with the documentation described below to HHS for review and approval (“Implementation Report”). The Implementation Report shall include:
1. An attestation signed by an officer of Lifespan attesting that the policies and procedures submitted to HHS under section V.B. and V.D. have been implemented;
 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 officer of Lifespan attesting that all members of the Lifespan workforce that use or disclose ePHI have completed training as required by this CAP and have executed the training certifications required by section V.E.2.;
 4. An attestation signed by an officer of Lifespan attesting that he or she has reviewed the Implementation Report, has made a reasonable inquiry regarding its content and believes, based upon such inquiry, that the information is accurate and truthful.

B. Annual Reports.

The one-year period beginning on the Effective Date and each subsequent one-year period during the course of the period of compliance obligations shall be referred to as “the Reporting Periods.” Lifespan also shall submit to HHS Annual Reports with respect to the status of and findings regarding Lifespan’s compliance with this CAP for each of the two (2) Reporting Periods. Lifespan 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 Lifespan 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 Reportable Events (defined in Section V.E.1) identified during the Reporting Period and the status of any corrective and preventative action relating to all such Reportable Events; and
4. An attestation signed by an owner or officer of Lifespan 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

Lifespan 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

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

A. Timely Written Requests for Extensions.

Lifespan 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 (5) days prior to the date such an act is required or due to be performed.

B. Notice of Breach of this CAP and Intent to Impose Civil Monetary Penalty.

The parties agree that a breach of this CAP by Lifespan constitutes a breach of the Agreement. Upon a determination by HHS that Lifespan has breached this CAP, HHS may notify Lifespan of: (1) Lifespan's breach; and (2) HHS' intent to impose a civil money penalty ("CMP") pursuant to 45 C.F.R. Part 160, or other remedies for the Covered Conduct 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. Lifespan's Response.


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

1. Lifespan is in compliance 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) Lifespan has begun to take action to cure the breach; (b) Lifespan is pursuing such action with due diligence; and (c) Lifespan 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, Lifespan fails to meet the requirements of section VIII.C. of this CAP to HHS' satisfaction, HHS may proceed with the imposition of a CMP against Lifespan pursuant to 45 C.F.R. Part 160 for any violations of the Covered Conduct 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 Lifespan in writing of its determination to proceed with the imposition of a CMP pursuant to 45 C.F.R. Part 160.

For Lifespan ACE



Paul J. Adler
Senior Vice President and General Counsel
Lifespan

June 26, 2020
Date

For United States Department of Health and Human Services



Susan M. Pezzullo Rhodes
Regional Manager, New England Region
Office for Civil Rights

June 26, 2020
Date