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. OSF Healthcare System and its Affiliated Covered Entities ("OSF") are covered entities, as defined at 45 C.F.R. § 160.103, and therefore are required to comply with the HIPAA Rules.

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

2. **Factual Background and Covered Conduct.**

   Pursuant to 45 C.F.R. § 164.408, OSF filed a breach notification report to HHS on October 1, 2021, describing that on April 23, 2021, OSF discovered evidence of files infected with the "Nephilim" variant of ransomware and a ransom note on its systems. Through its investigation, OSF determined, on August 24, 2021, that the threat actors stole the protected health information (PHI) of 53,907 patients. OSF notified the patients and HHS on October 1, 2021. In response, HHS began an investigation.

   HHS's investigation included assessing OSF's compliance with the applicable Federal Standards for Privacy of Individually Identifiable Health Information and/or the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160 and 164, Subparts A, C, and E, the Privacy and Security Rules), and the Breach Notification Rule (45 C.F.R. Parts 160 and 164, Subpart D).

   HHS' investigation indicated that the following conduct occurred (Covered Conduct):

   a. OSF failed to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to ePHI held by OSF. *See* 45C.F.R. § 164.308(a)(1)(ii)(A);

b. As a result of stolen data obtained in a ransomware attack, OSF impermissibly disclosed the PHI of 53,907 individuals. *See* 45 C.F.R. § 164.502(a);

c. OSF failed to provide timely notification to individuals affected by the breach. *See* 45 C.F.R. § 164.404(b); and

d. OSF failed to provide timely notification to the Secretary of HHS that the 2021 ransomware attack resulted in the disclosure of 500 or more individuals' PHI. *See* 45 C.F.R. § 164.408(b).

No Admission. This Agreement is not an admission of liability by OSF, an admission that it violated any HIPAA Rules or that it is liable for any civil money penalties.

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

4. **Intention of Parties to Effect Resolution.** This Agreement is intended to resolve OCR Transaction Number 22-445707 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

5. **Payment.** HHS has agreed to accept, and OSF has agreed to pay HHS, the amount of **$552,250** ("Resolution Amount"). OSF agrees to pay the Resolution Amount in one lump sum by July 15, 2026, by automated clearing house transaction pursuant to written instructions to be provided by HHS.

6. **Corrective Action Plan.** OSF 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 OSF breaches the CAP and fails to cure the breach as set forth in the CAP, then OSF 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.

7. **Release by HHS.** In consideration of and conditioned upon OSF's performance of its obligations under this Agreement, HHS releases OSF from any actions it may have against OSF under the HIPAA Rules arising out of or related to the Covered Conduct identified in paragraph I.2 of this Agreement. HHS does not release OSF 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.

8. **Agreement by Released Party.** OSF 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. OSF 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.

9. **Binding on Successors.** This Agreement is binding on OSF and its successors, heirs, transferees, and assigns.

10. **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.

11. **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.

12. **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.

13. **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").

14. **Tolling of Statute of Limitations.** Pursuant to 42 U.S.C. § 1320a-7a(c)(1), a civil money 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, OSF agrees that the time between the Effective Date of this Agreement (as set forth in Paragraph 13) and the date the Agreement may be terminated by reason of OSF'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. OSF 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.

15. **Disclosure.** HHS places no restriction on the publication of the Agreement. This Agreement and information related to this Agreement may be made public by either Party.

16. **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.

17. **Authorizations.** The individual(s) signing this Agreement on behalf of OSF represent and warrant that they are authorized by OSF 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.

[SIGNATURES ON FOLLOWING PAGE]

For OSF Healthcare System

Gina A. Thompson

Gina Arnett Thompson
Chief Integrity Officer
OSF Healthcare System

7/1/2026
Date

For the United States Department of Health and Human Services

Jamie R Ballay

Jamie Rahn Ballay
Regional Manager
Office for Civil Rights

July 1, 2026
Date

Appendix A

CORRECTIVE ACTION PLAN
BETWEEN THE
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES AND
OSF HEALTHCARE SYSTEM

I. Preamble

OSF Healthcare System ("OSF") 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, OSF is entering into a Resolution Agreement ("Agreement") with HHS, and this CAP is incorporated by reference into the Agreement as Appendix A. OSF enters into this CAP as part of the consideration for the release set forth in paragraph II.7 of the Agreement.

II. Contact Persons and Submissions

A. Contact Persons.

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

Gina Arnett Thompson
SVP, Chief Integrity Officer
OSF HealthCare System
Compliance and Internal Audit Division
124 SW Adams Street
Peoria, IL 61602
Phone (309) 308-5960
Gina.Thompson@osfhealthcare.org

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

Amy Kaplan
Office for Civil Rights
U.S. Department of Health and Human Services
801 Market Street, Suite 9300
Philadelphia, PA 19107-3134
(215) 861-4446
Amy.Kaplan@hhs.gov

OSF 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. 13 of the Agreement ("Effective Date"). The period for compliance ("Compliance Term") with the obligations assumed by OSF 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 OSF under section VIII hereof of its determination that OSF has breached this CAP. In the event of such a notification by HHS under section VIII hereof, the Compliance Term shall not end until HHS notifies OSF that it has determined that the breach has been cured. After the Compliance Term ends, OSF 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 OSF'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

OSF agrees to the following:

A. Conduct a Risk Analysis.

1. OSF shall conduct an accurate and thorough risk analysis of the security threats to, and vulnerabilities of, its electronic protected health information (ePHI) that incorporates all electronic equipment, data systems, programs and applications controlled, administered, owned, or shared by OSF or any affiliates that are owned, controlled, or managed by OSF. As part of this process, OSF shall develop a complete inventory of all electronic equipment, data systems, off-site data storage facilities, and applications, including, if applicable, web technology deployed on OSF webpages, that create, receive, maintain, or transmit ePHI, which will then be incorporated in its risk analysis.

2. Within sixty (60) calendar days of the Effective Date, OSF shall submit to HHS the scope and methodology by which it proposes to conduct the risk analysis. HHS shall notify OSF whether the proposed scope and methodology is or is not consistent with 45 C.F.R. § 164.308 (a)(l)(ii)(A).

3. OSF shall provide the risk analysis to HHS within ninety (90) calendar days of HHS' approval of the scope and methodology for HHS' review.

4. Upon submission by OSF, HHS shall review and recommend changes to the aforementioned risk analysis. Upon receiving HHS' recommended changes, OSF 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.

5. OSF shall annually conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by OSF. A subsequent risk analysis shall be submitted for review by HHS in the same manner as described in this section until the conclusion of the CAP, for a total of two risk analyses during the term of the CAP.

B. Develop and Implement a Risk Management Plan

1. OSF 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 OSF's implementation, evaluation, and revision of its risk remediation activities.

2. Within ninety (90) calendar days of HHS' final approval of the risk analysis described in section V.A.1 above, OSF shall submit a risk management plan to HHS for HHS' review and approval. HHS shall approve, or, if necessary, require revisions to OSF's risk management plan.

3. Upon receiving HHS' notice of required revisions, if any, OSF shall have thirty (30) calendar 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) calendar days of HHS' approval of the risk management plan, OSF shall finalize and officially adopt the risk management plan in accordance with its applicable administrative procedures.

C. Reportable Events

1. During the Compliance Term, OSF shall, upon learning that a workforce member likely failed to comply with its existing policies and procedures, promptly investigate this matter. If OSF, after review and investigation, determines that a member of its workforce has failed to comply with its policies and procedures, OSF shall report such events to HHS as provided in Section VI. 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 OSF's Privacy, Security, and Breach Notification policies and procedures; and

    b. A description of the actions taken and any further steps OSF 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 Privacy, Security, and Breach Notification policies and procedures.

    c. If no Reportable Events occur during the Compliance Term, OSF shall so inform HHS in the Annual Report(s) as specified in Section VI below.

VI. Annual Reports

A. Annual Reports.

1. The one (1) year period after the Effective Date and each subsequent one (1) year period during the course of the Compliance Term shall be known as a "Reporting Period." Within sixty (60) calendar days after the close of each corresponding Reporting Period, OSF shall submit a report to HHS regarding OSF's compliance with this CAP for each corresponding Reporting Period ("Annual Report"). The Annual Report shall include:

    a. An attestation signed by an owner or officer of OSF attesting that all members of the workforce have completed the HIPAA training required by HIPAA during the Reporting Period, or are in the process of completing the training. For workforce members who have not completed the training, the attestation will state the number of workforce members that have not completed the training, and the timeframe for when all of those workforce members will complete the training.

    b. A summary of Reportable Events (defined in V.C), if any, the status of any corrective and preventative action(s) relating to all such Reportable Events, or an attestation signed by an officer or director of OSF stating

that no Reportable Events occurred during the Compliance Term.

c. An attestation signed by an owner or officer of OSF 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

OSF 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. Requests for Extensions and Breach Provisions

A. Timely Written Requests for Extensions. OSF 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) calendar days prior to the date such an act is required or due to be performed. This requirement may be waived by HHS 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 OSF constitutes a breach of the Agreement. Upon a determination by HHS that OSF has breached this CAP, HHS may notify OSF of: (1) OSF's breach; and (2) HHS' intent to impose a 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 for any other conduct that constitutes a violation of the HIPAA Privacy, Security, and Breach Notification Rules ("Notice of Breach and Intent to Impose CMP").

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

1. OSF 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 30-day period, but that: (a) OSF has begun to take action to cure the breach; (b) OSF is pursuing such action with due diligence; and (c) OSF has provided to HHS a reasonable timetable for curing the breach.

D. Imposition of CMP. If at the conclusion of the 30-day period, OSF fails to meet the requirements of this CAP to HHS' satisfaction, HHS may proceed with the imposition of the CMP against OSF pursuant to 45 C.F.R. Part 160 for any violations of the Covered Conduct set forth in paragraph 1.2 of the Agreement and for any other act or

failure to act that constitutes a violation of the HIPAA Rules. HHS shall notify OSF in writing of its determination to proceed with the imposition of the CMP.

For OSF Healthcare System

Gina A. Thompson

Gina Arnett Thompson
Chief Integrity Officer
OSF Healthcare System

7/1/2026
Date

For the United States Department of Health and Human Services

Jamie R Ballay

Jamie Rahn Ballay
Regional Manager
Office for Civil Rights

July 1, 2026
Date