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. Lifetime Healthcare, Inc., which, for purposes of this Agreement, includes its affiliates, Excellus Health Plan, Inc., doing business as Excellus BlueCross BlueShield and Univera Healthcare, a New York not-for-profit health service corporation that provides health care coverage to 1.5 million individuals in Upstate and Western New York, The MedAmerica Companies (MedAmerica Insurance Company, MedAmerica Insurance Company of Florida, and MedAmerica Insurance Company of New York), and Lifetime Benefit Solutions, Inc.; its dissolved affiliate, Genesee Valley Group Health Association, formerly doing business as Lifetime Health Medical Group; and its former affiliate, Genesee Region Home Care Association, Inc., doing business as Lifetime Care (all, collectively, referred to as "EHP"), is 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 EHP shall together be referred to herein as the "Parties."

2. Factual Background and Covered Conduct.

On September 9, 2015, HHS received a breach report from EHP, notifying HHS that cyberattackers had gained unauthorized access to its information technology systems that included electronic protected health information (ePHI) for approximately 10 million[1] individuals. On June 29, 2016, HHS notified EHP that it was initiating an investigation regarding

[1] EHP advised OCR that the final number of potentially affected individuals is 9,358,891.

EHP's compliance with the Privacy, Security and Breach Notification Rules. HHS' investigation indicated potential violations of the following provisions ("Covered Conduct"):

a. The requirement to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of its ePHI (*See* 45 C.F.R. § 164.308(a)(1)(ii)(A)).

b. The requirement to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a) (*See* 45 C.F.R. § 164.308(a)(1)(ii)(B)).

c. The requirement to implement procedures to regularly review records of information system activity (*See* 45 C.F.R. § 164.308(a)(1)(ii)(D)).

d. The requirement to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4) (*See* 45 C.F.R. § 164.312(a)(1)).

e. The requirement to prevent unauthorized access to the ePHI of 9,358,891 individuals whose ePHI was maintained in EHP's IT systems(*See* 45 C.F.R. § 164.502(a)).

3. No Admission. This Agreement is not an admission, concession, or evidence of liability by EHP.

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

5. Intention of Parties to Effect Resolution. This Agreement is intended to resolve OCR Transaction Number: 15-219607 and any potential violations of the HIPAA Rules related to the Covered Conduct specified in section I.2 of this Agreement. In consideration of the Parties' interest in avoiding the uncertainty, burden, and expense of 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 EHP has agreed to pay HHS, the amount of **$5,100,000** ("Resolution Amount"). EHP agrees to pay the Resolution Amount on or before February 12, 2021, pursuant to written instructions to be provided by HHS.

7. Corrective Action Plan. EHP 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 EHP breaches the CAP, and fails to cure the breach as set forth in

the CAP, then EHP 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 EHP's performance of its obligations under this Agreement, HHS releases EHP from any actions it may have against EHP under the HIPAA Rules arising out of or related to the Factual Background and Covered Conduct identified in section I.2 of this Agreement. HHS does not release EHP 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. EHP 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. EHP 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 EHP 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, EHP 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 EHP 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. EHP waives and will not plead any statute of limitations,

laches, or similar defenses to any administrative action relating to the covered conduct identified in section 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 EHP represent and warrant that they are authorized by EHP 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 Covered Entity

/s/ 1/14/2021

Barry Thornton Date
Chief Operating Officer
Excellus Health Plan, Inc.

For the United States Department of Health and Human Services

/s/ 1/15/2021

Linda C. Colón Date
Regional Manager
Eastern and Caribbean Region
Office for Civil Rights

Appendix A

CORRECTIVE ACTION PLAN

BETWEEN THE

DEPARTMENT OF HEALTH AND HUMAN SERVICES

AND

EXCELLUS HEALTH PLAN, INC.

I. Preamble

Excellus Health Plan, Inc. (hereinafter known as "EHP") 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, EHP is entering into a Resolution Agreement ("Agreement") with HHS, and this CAP is incorporated by reference into the Resolution Agreement as Appendix A. EHP enters into this CAP as part of consideration for the release set forth in section II.8 of the Agreement.

II. Contact Persons and Submissions

A. Contact Persons

EHP has identified the following individuals as its authorized representatives and contact persons regarding the implementation of this CAP and for receipt and submission of notifications and reports:

Bruce Jones, Chief Information Officer
Excellus Health Plan, Inc.
165 Court Street
Rochester, New York 14647
Voice Phone (585) 530-5511
bruce.jones@excellus.com

Timothy J. Quinlivan, General Counsel
Excellus Health Plan, Inc.
165 Court Street
Rochester, New York 14647
Voice Phone (585) 530-6788
timothy.quinlivan@excellus.com

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

Linda C. Colón, Regional Manager
Eastern and Caribbean Region
Office for Civil Rights
U.S. Department of Health and Human Services
26 Federal Plaza, Suite 3312
New York, New York 10278
Voice Phone (212) 264-4136
Fax: (212) 264-3039

EHP 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, hand delivery, email, or secure FTP transfer, 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 EHP under this CAP shall begin on the Effective Date of this CAP and end two (2) years from the Effective Date, unless before the end of the two (2) year period, HHS has notified EHP under section VIII.B hereof of its position that EHP breached this CAP. In the event of such a notification by HHS under section VIII.B hereof, the Compliance Term shall not end until HHS either (1) notifies EHP that it has determined that the breach has been cured or (2) notifies EHP under VIII.D hereof that it will seek imposition of a CMP. After the Compliance Term ends, EHP 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 EHP'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

EHP agrees to the following:

A. Security Management Process

1. EHP shall conduct a comprehensive and thorough Risk Analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by EHP. This Risk Analysis shall incorporate all EHP facilities, whether owned or rented, and evaluate the risks to the ePHI on all of its electronic equipment, data systems, and applications controlled, administered or owned by EHP or any EHP entity, that contain, store, transmit, or receive ePHI. Prior to conducting the Risk Analysis, EHP shall develop a complete inventory of all of its facilities, electronic equipment, data systems, and applications that contain or store ePHI that will then be incorporated into its Risk Analysis. EHP may submit a Risk Analysis currently underway for consideration by HHS for compliance with this provision.

2. EHP shall provide the Risk Analysis, consistent with section V.A.1, to HHS within one hundred eighty (180) days of the Effective Date for HHS' review. Within sixty (60) days of its receipt of EHP's Risk Analysis, HHS will inform EHP whether HHS approves or disapproves of the Risk Analysis. If HHS disapproves of the Risk Analysis, HHS shall provide EHP with technical assistance, as necessary, regarding the basis for disapproval so that EHP may prepare a revised Risk Analysis. EHP shall have sixty (60) days in which to revise its Risk Analysis accordingly, and then submit the revised Risk Analysis to HHS for review and approval. This submission and review process shall continue until HHS approves the Risk Analysis.

3. EHP shall develop an enterprise-wide Risk Management Plan to address and mitigate any security risks and vulnerabilities found in the Risk Analysis described above. The Risk Management Plan shall include a process and timeline for EHP's implementation, evaluation, and revision of its risk remediation activities. EHP may submit a Risk Management Plan currently underway for consideration by HHS for compliance with this provision.

4. Within ninety (90) days of HHS' final approval of the Risk Analysis described in section V.A above, EHP shall submit EHP's Risk Management Plan to HHS for HHS' review. Within sixty (60) days of its receipt of EHP's Risk Management Plan, HHS will inform EHP whether HHS approves the Risk Management Plan or HHS requires revisions. If HHS requires revisions to the Risk Management Plan, HHS shall provide EHP with a written explanation of the basis of its revisions, including comments and recommendation that EHP can use to prepare a revised Risk Management Plan. Upon receiving HHS's notice of required revisions, if any, EHP shall have sixty (60) days in which to revise its Risk Management Plan accordingly, and submit the revised Risk Management Plan to HHS for review and approval. This submission and review process shall continue until HHS approves the Risk Management Plan. Within thirty (30) days of HHS' approval of the Risk Management Plan, EHP shall finalize and officially adopt the Risk Management Plan in accordance with its applicable administrative procedures and distribute the plan to workforce members involved with implementation of the plan.

B. Policies and Procedures

1. EHP shall review, and as necessary, develop maintain, and revise the written policies and procedures to addressing the Minimum Content set forth in Section V.D. to confirm compliance with the Federal standards that govern the privacy and security of individually identifiable health information (45 C.F.R. Part 160 and 164, Subpart C (the Security Rule").

2. EHP shall provide the policies and procedures identified in section V.B.1 above to HHS for review and approval within sixty (60) days of HHS' approval of its risk analysis, as required by V.A.2. Upon receiving any recommended changes to such policies and procedures from HHS, EHP shall have forty-five (45) days to revise such policies and procedures accordingly and provide the revised policies and procedures to HHS for review and approval. This process shall continue until HHS approves such policies and procedures.

3. EHP shall adopt (in accordance with its applicable administrative procedures) the policies and procedures approved by HHS pursuant to section V.B.2 within ninety (90) days of receipt of HHS' approval.

C. Distribution and Updating of Policies and Procedures

1. EHP shall make available, for example through publication on its Intranet, the policies and procedures identified in section V.B. to all members of the EHP's workforce subject to those policies and procedures who use or disclose ePHI within thirty (30) days EHP's adoption of such policies and procedures, and thereafter to new members of the workforce subject to those policies and procedures and who will use or disclose ePHI within thirty (30) days of their beginning of service.

D. Minimum Content of the Policies and Procedures

1. The Policies and Procedures subject to his CAP shall include and be limited to policies and procedures that address the following Security Rule provisions:

a. Information system activity review for the regular review of audit logs, access reports, and security incident tracking reports to monitor and respond to suspicious events pursuant to 45 C.F.R. § 164.308(a)(1)(ii)(D). This includes parameters for reviewing systems' activity, the frequency of the reviews and procedures for documenting and reporting results of such reviews.

b. Access Control – 45 C.F.R. § 164.312(a)(1), including provisions to address access between systems, such as network or portal segmentation, provisions to limit access to ePHI to individuals and software programs granted access rights, and provisions to enforce password management requirements, such as password age.

E. Reportable Events

1. During the Compliance Term, in the event that EHP receives information that a workforce member subject to the policies and procedures under section V.B.3 may have failed to comply with those policies and procedures, EHP shall promptly investigate this matter. If EHP determines, after such investigation, that during the Compliance Term a member of its workforce subject to the policies and procedures adopted by EHP under section V.B.3 failed to comply with those policies and procedures, and such failure was material (e.g. a violation that results in a presumed Breach of Unsecured PHI), EHP 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 description of the event, including the relevant facts, the persons involved, and the provision(s) of the policies and procedures under section V.B. implicated; and

b. A description of the actions taken and any further steps EHP plans to take to address the matter to mitigate any harm, and to prevent it from recurring, including sanctions, if any.

2. If no Reportable Events occur within the Compliance Term, EHP shall so inform HHS in its 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 HHS approves Policies and Procedures specified in section V.B. above, EHP 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 EHP attesting that the policies and procedures submitted to HHS under section V.B. have been implemented; and

2. An attestation signed by an officer of EHP 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." EHP also shall submit to HHS Annual Reports with respect to the status of and findings regarding EHP's compliance with this CAP for each of the two (2) Reporting Periods. EHP 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 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;

2. An attestation signed by an officer of EHP 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

EHP 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

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

A. Timely Written Requests for Extensions

EHP 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 Money Penalty

The Parties agree that a breach of this CAP by EHP constitutes a breach of the Agreement. Upon a determination by HHS that EHP has breached this CAP, HHS may notify EHP via email and overnight hardcopy delivery of: (1) its belief that EHP has breached the agreement and the basis thereof; and (2) HHS' intent to impose a CMP pursuant to 45 C.F.R. Part 160, for the Covered Conduct set forth in section I.2 of the Agreement ("Notice of Breach and Intent to Impose CMP"), including the amount of such CMP.

C. EHP's Response

EHP 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. EHP 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) EHP has begun to take action to cure the breach; (b) EHP is pursuing such action with due diligence; and (c) EHP has provided HHS a reasonable timetable for curing the breach.

D. Imposition of CMP

If at the conclusion of the thirty (30) day period, EHP 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 EHP pursuant to 45 C.F.R. Part 160 for any violations of the HIPAA Rules related to the Covered Conduct set forth in section I.2 of the Agreement. HHS shall promptly notify EHP in writing of its determination to proceed with the imposition of a CMP pursuant to

45 C.F.R. Part 160. HHS must offset any CMP amount levied under this section by the amounts already paid by EHP in lieu of CMPs under this Resolution Agreement. Any such offset will apply only to Covered Conduct up to and including the Effective Date.

For Excellus Health Plan, Inc.

/s/ 1/14/2021

Barry Thornton
Chief Operating Officer
Excellus Health Plan, Inc.

Date

For United States Department of Health and Human Services

/s/ 1/15/2021

Linda C. Colón
Regional Manager
Eastern and Caribbean Region
Office for Civil Rights

Date