

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. Cancer Care Group, P.C. (“CCG”) which is a covered entity, as defined at 45 C.F.R. § 160.103, and therefore is required to comply with the HIPAA Rules. CCG is one of the largest radiation oncology private physician practices in the country, and its physicians focus on the use of radiation therapy in the treatment and management of cancer.

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

2. Factual Background and Covered Conduct.

On August 29, 2012, HHS received notification from CCG regarding a breach involving unsecured electronic protected health information (ePHI). CCG reported that, on July 19, 2012, a laptop bag was stolen from an employee’s car in Indianapolis, Indiana. According to the report, the laptop bag contained the employee’s computer, which did not contain ePHI, and computer server backup media, which contained the ePHI of approximately 55,000 individuals. During the course of its investigation, OCR learned that a CCG workforce member left the computer server backup media, which was unencrypted, unattended in the passenger section of the workforce member’s car, where it was then stolen by a third party who broke a window to obtain access to the inside of the car.

OCR’s investigation indicated that the following covered conduct occurred:

A. From April 21, 2005, the compliance date of the Security Rule, until November 5, 2012, CCG failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality

integrity, and availability of ePHI held by CCG (*See* 45 C.F.R. § 164.308(a)(1)(ii)(A));

- B. From April 21, 2005, the compliance date of the Security Rule, until January 22, 2013, CCG failed to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility (*See* 45 C.F.R. § 164.310(d)(1)); and
- C. On July 19, 2012, CCG impermissibly disclosed the ePHI of approximately 55,000 individuals by providing access to the ePHI to an unauthorized individual for a purpose not permitted by the Privacy Rule when it failed to safeguard unencrypted back-up tapes that were stolen from the unattended vehicle of one of its workforce members (*See* 45 C.F.R. § 164.502(a)).

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

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

5. Intention of Parties to Effect Resolution. This Agreement is intended to resolve OCR Transaction Number 13-150947 regarding potential 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, and in consideration and furtherance of CCG's voluntary corrective actions following the breach of ePHI, 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 CCG has agreed to pay HHS, the amount of \$750,000 ("Resolution Amount") as further remediation of this matter. CCG agrees to pay the Resolution Amount on the Effective Date of this Agreement as defined in paragraph II.14 by automated clearing house transaction pursuant to written instructions to be provided by HHS.

7. Corrective Action Plan. CCG 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 CCG breaches the CAP, and fails to cure the breach as set forth in the CAP, then CCG 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 CCG's performance of its obligations under this Agreement, HHS releases CCG from any actions it may have against CCG 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 CCG 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. CCG 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. CCG 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 CCG 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 civil money penalty (“CMP”) must be imposed within six 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, CCG agrees that the time between the Effective Date of this Agreement and the date the Agreement may be terminated by reason of CCG’s breach, plus one-year thereafter, will not be included in calculating the six (6) year statute of limitations applicable to the potential violations which are the subject of this Agreement. CCG 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. 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 CCG represent and warrant that they are authorized by CCG 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 Cancer Care Group, P.C.

/S/

08/31/2015

Thomas Dugan, M.D.
President
Cancer Care Group, P.C.

Date

For United States Department of Health and Human Services

/S/

08/31/2015

Celeste H. Davis, Esq.
Regional Manager, Region V
Office for Civil Rights

Date

Appendix A
CORRECTIVE ACTION PLAN
BETWEEN THE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
AND
CANCER CARE GROUP, P.C.

I. Preamble

Cancer Care Group, P.C. (hereinafter known as “CCG”) 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, CCG is entering into a Resolution Agreement (“Agreement”) with HHS, and this CAP is incorporated by reference into the Resolution Agreement as Appendix A. CCG 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

CCG 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:

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

CCG 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 CCG under this CAP shall begin on the Effective Date of this CAP and end three (3) years from the Effective Date unless HHS has notified CCG under section VIII hereof of its determination that CCG 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 CCG that it has determined that the breach has been cured. After the Compliance Term ends, CCG shall still be obligated to submit the final Annual Report as required by section VI and comply with the document retention requirement in section VII.

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

CCG agrees to the following:

A. Conduct Risk Analysis.

1. CCG shall conduct a current, comprehensive and thorough Risk Analysis of security risks and vulnerabilities that incorporates its current facility or facilities and the electronic equipment, data systems, and applications controlled, currently administered or owned by CCG, that contain, store, transmit, or receive electronic protected health information (“ePHI”). Upon CCG’s completion, CCG shall submit the Risk Analysis to HHS for HHS’ review, and either approval or disapproval, consistent with section V.A.2, below.

2. CCG shall provide such Risk Analysis, consistent with section V.A.1 above, to HHS within ninety (90) days of the Effective Date for HHS’ review and either approval or disapproval. Within sixty (60) days of its receipt of CCG’s Risk Analysis, HHS will inform CCG in writing as to whether HHS approves or disapproves of the Risk Analysis. If HHS disapproves of the Risk Analysis, HHS shall provide CCG with a detailed, written explanation of

the basis of its disapproval, including comments and recommendations that CCG can use to prepare a revised Risk Analysis. Upon receiving a disapproval of the Risk Analysis from HHS, and a description of any required changes to the Risk Analysis, CCG 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 or disapproval. This process shall continue until HHS approves the Risk Analysis.

3. CCG shall review the Risk Analysis annually (or more frequently, if appropriate) and shall promptly update the Risk Analysis in response to environmental or operational changes affecting the security of electronic protected health information. Following an update to the Risk Analysis, CCG shall assess whether its existing security measures are sufficient to protect its electronic protected health information, and revise its Risk Management Plan, Policies and Procedures, training materials, and implement additional security measures, as needed.

B. Develop and Implement Risk Management Plan.

1. CCG shall develop an organization-wide Risk Management Plan to address and mitigate any security risks and vulnerabilities found in the Risk Analysis described in section V.A. above. The Risk Management Plan shall include a process and timeline for CCG's implementation, evaluation, and revision of its risk remediation activities. The Risk Management Plan shall be forwarded to HHS for its review, and either approval or disapproval, consistent with section V.B.2, below.

2. Within ninety (90) days of HHS' final approval of the Risk Analysis described in section V.A. above, CCG shall submit its Risk Management Plan to HHS for HHS' review and either approval or disapproval. Within sixty (60) days of its receipt of CCG's Risk Management Plan, HHS will inform CCG in writing as to whether HHS approves or disapproves of the Risk Management Plan. If HHS disapproves of the Risk Management Plan, HHS shall provide CCG with detailed comments and recommendations so that CCG can prepare a revised Risk Management Plan. Upon receiving any required changes to such Risk Management Plan from HHS, CCG shall have sixty (60) days in which to revise its Risk Management Plan accordingly, and then submit the revised Risk Management Plan to HHS for review and approval or disapproval. This submission and review process shall continue until HHS approves the Risk Management Plan.

3. Within sixty (60) days of HHS' approval of the Risk Management Plan, CCG shall begin implementation of the Risk Management Plan.

C. Review and Revise Policies and Procedures.

1. CCG shall review and, to the extent necessary, revise, its current Security Rule Policies and Procedures ("Policies and Procedures") based on the findings of the Risk Analysis and the implementation of the Risk Management Plan, as required by sections V.A and V.B, respectively. CCG's Policies and Procedures must comply with the HIPAA Security Rule. The revised Policies and Procedures, if any, shall be forwarded to HHS for its review, and either approval or disapproval, consistent with section V.C.2, below.

2. If applicable, CCG shall provide such revised Policies and Procedures, consistent with section V.C.1 above, to HHS within sixty (60) days of the HHS's final approval of the Risk Management Plan described in section V.B above, for HHS' review and either approval or disapproval. Within thirty (30) days of its receipt of CCG's revised Policies and Procedures, HHS will inform CCG in writing as to whether HHS approves or disapproves of the Policies and Procedures. If HHS disapproves of the Policies and Procedures, HHS shall provide CCG with a detailed, written explanation of the basis of its disapproval, including comments and recommendations that CCG can use to further revise the Policies and Procedures. Upon receiving a disapproval of the Policies and Procedures from HHS, and a description of any required changes to the Policies and Procedures, CCG shall have thirty (30) days in which to revise its Policies and Procedures accordingly, and then submit the revised Policies and Procedures to HHS for review and approval or disapproval. This process shall continue until HHS approves the Policies and Procedures.

3. Within thirty (30) days of HHS' approval of the Policies and Procedures, CCG shall begin implementation of the Policies and Procedures and shall distribute the approved Policies and Procedures to the relevant and appropriate CCG workforce members.

D. Review and Revise Training Program.

1. CCG shall review and, to the extent necessary, revise, its current Security Rule Training Program (Training Program) based on the findings of the Risk Analysis and the implementation of the Risk Management Plan, as required by sections V.A and V.B, respectively, above, as well as any revisions to the Policies and Procedures, as described in section V.C, above. CCG's Training Program must comply with the HIPAA Security Rule. The revised Training Program, if applicable, shall be forwarded to HHS for its review, and either approval or disapproval, consistent with section V.D.2, below.

2. If applicable, CCG shall provide the revised Training Program, consistent with section V.D.1, above, to HHS within sixty (60) days of the HHS's final approval of the revised Policies and Procedures, described in section V.C above, for HHS' review and either approval or disapproval. Within thirty (30) days of its receipt of CCG's revised Training Program, HHS will inform CCG in writing as to whether HHS approves or disapproves of the Training Program. If HHS disapproves of the Training Program, HHS shall provide CCG with a detailed, written explanation of the basis of its disapproval, including comments and recommendations that CCG can use to further revise the Training Program. Upon receiving a disapproval of the Training Program from HHS, and a description of any required changes to the Training Program, CCG shall have thirty (30) days in which to revise its Training Program accordingly, and then submit the revised Training Program to HHS for review and approval or disapproval. This process shall continue until HHS approves the Training Program.

3. Within thirty (30) days of HHS' approval of the Training Program, CCG shall begin implementation of the Training Program and shall administer the approved Training Program to all members of CCG's workforce who have access to and use ePHI.

E. Reportable Events. During the Compliance Term, CCG shall, upon receiving information that a workforce member may have failed to comply with its Policies and

Procedures, promptly investigate the matter. If CCG determines, after review and investigation, that a member of its workforce has failed to comply with these policies and procedures, CCG shall notify HHS in writing within thirty (30) days. Such violations shall be known as Reportable Events. The report to HHS shall include the following information

1. A complete description of the event, including the relevant facts, the persons involved, and the provision(s) of the policies and procedures implicated; and

2. A description of the actions taken and any further steps CCG 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 its Policies and Procedures.

VI. Annual Reports

A. 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.” CCG shall submit to HHS Annual Reports with respect to the status of and findings regarding CCG’s compliance with this CAP for each of the three (3) Reporting Periods. CCG shall submit each Annual Report to HHS no later than thirty (30) days after the end of each corresponding Reporting Period. The final report shall be due thirty (30) days after CCG’s obligations under the CAP are otherwise concluded. The Annual Report shall include:

1. A detailed description of updates or changes, if any, to the risk analysis or risk management plan made pursuant to section V.A.3. This shall include a summary of CCG’s strategy related to the assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by CCG; the identification of all outside entities assisting CCG in this process; and documentation related to the security measures CCG implemented or is implementing, if any, to sufficiently reduce the identified risks and vulnerabilities to a reasonable and appropriate level;

2. A detailed description of any revisions to CCG’s Policies and Procedures and training materials, if any, made pursuant to section V.A.3;

3. A summary of Reportable Events, as defined in section V.E, if any, 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 CCG 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

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

VIII. Breach Provisions

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

A. Timely Written Requests for Extensions. CCG 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 CCG constitutes a breach of the Agreement. Upon a determination by HHS that CCG has breached this CAP, HHS may notify CCG of: (1) CCG’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. CCG’s Response. CCG 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. CCG 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) CCG has begun to take action to cure the breach; (b) CCG is pursuing such action with due diligence; and (c) CCG has provided to HHS a reasonable timetable for curing the breach.

D. Imposition of CMP. If at the conclusion of the 30-day period, CCG 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 CCG 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 CCG in writing of its determination to proceed with the imposition of a CMP.

For Cancer Care Group, P.C.

/S/

08/31/2015

Thomas Dugan, M.D.
President
Cancer Care Group, P.C.

Date

For United States Department of Health and Human Services

/S/

08/31/2015

Celeste H. Davis, Esq.
Regional Manager – Region V
Office for Civil Rights

Date