

ANDREW J. BRUCK
ACTING ATTORNEY GENERAL OF NEW JERSEY
Division of Law
124 Halsey Street, 5th Floor
P.O. Box 45029
Newark, New Jersey 07101
Attorney for the New Jersey Division of Consumer Affairs

FILED

December 15 2021

Division of Consumer Affairs

By: Gina F. Pittore
Deputy Attorney General
(973) 648- 4137

STATE OF NEW JERSEY
DEPARTMENT OF LAW AND PUBLIC
SAFETY DIVISION OF CONSUMER AFFAIRS

In the Matter of

RCCA MSO LLC, Regional Cancer Care
Associates LLC, and RCCA MD LLC,

Respondents.

Administrative Action

CONSENT ORDER

WHEREAS this matter having been opened by the New Jersey Division of Consumer Affairs, Office of Consumer Protection, as an investigation to ascertain whether violations of the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 to -226 (“CFA”), the New Jersey Identity Theft Prevention Act, N.J.S.A. 56:8-161 to -166 (“ITPA”), and/or the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, and the Department of Health and Human Services Regulations, 45 C.F.R. § 160 to 180 (collectively, “HIPAA”) have been or are being committed (the “Investigation”) by RCCA MSO LLC, Regional Cancer Care Associates LLC, and RCCA MD LLC (collectively, “RCCA” or “Respondents”);

WHEREAS the Attorney General is charged with the responsibility of enforcing the CFA and the ITPA, and the Director of the Division is charged with administering the CFA on behalf of the Attorney General;

WHEREAS the Attorney General, as *parens patriae* for the State of New Jersey and in its sovereign capacity, may, pursuant to 42 U.S.C. § 1320d-5(d), enforce the provisions of HIPAA;

WHEREAS Respondents are all New Jersey-based companies incorporated in New Jersey, and headquartered at 25 Main Street, Hackensack, New Jersey;

WHEREAS RCCA has thirty (30) locations in New Jersey, Maryland, and Connecticut that provide cancer care treatment and related services;

WHEREAS the Division alleges that RCCA engaged in conduct that violated the CFA and HIPAA in connection with the improper handling of, and unreasonable security measures implemented to secure Personal Information, Protected Healthcare Information, and/or Electronic Protected Healthcare Information stored on its employee email accounts from approximately April 17, 2019, through June 4, 2019, affecting 105,200 consumers nationwide, including 80,333 New Jersey residents;

WHEREAS the Division alleges that RCCA engaged in conduct that violated the CFA and HIPAA in connection with the improper disclosure of Personal Information, Protected Healthcare Information, and/or Electronic Protected Healthcare Information discovered on July 25, 2019, affecting 13,047 consumers nationwide; and

WHEREAS the Division and RCCA (collectively, the “Parties”) have reached an amicable agreement resolving the issues in controversy and concluding the Investigation without the need for further action, and RCCA having cooperated with the Investigation and consented to the entry of the within order (“Consent Order”) without admitting any violation of law, and for

good cause shown;

IT IS ORDERED AND AGREED as follows:

1. EFFECTIVE DATE

1.1. This Consent Order is effective on the date that it is filed with the Division, which filing date the Division Clerk stamps on the executed Consent Order (“Effective Date”).

2. DEFINITIONS

Unless otherwise defined herein, the following words or terms shall have the following meanings for purposes of this Consent Order:

2.1. “Atlantic” shall refer to Facsimile Communications Industries Inc. d/b/a Atlantic Tomorrow’s Office, an information technology service provider with whom RCCA entered into a Managed Service Agreement on February 1, 2017.

2.2. “Attorney General” shall refer to the Attorney General of the State of New Jersey and the Office of the Attorney General of the State of New Jersey.

2.3. “Breach Notification Rule” shall refer to 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and D.

2.4. “Business Associate” shall be defined in accordance with 45 C.F.R. § 160.103.

2.5. “Business Associate Agreement” or “BAA” shall mean the contract or other written arrangement required by 45 C.F.R. § 164.502(e)(2) and meeting the requirements of 45 C.F.R. §164.504(e).

2.6. “Covered Entity” shall be defined in accordance with 45 C.F.R. § 160.103.

2.7. “Covered Systems” shall mean components, such as servers, workstations, and devices, within the RCCA Network that are routinely used to collect, process, communicate, and/or store PI and/or ePHI.

2.8. “Cyber Security Operations Center” or “C-SOC” shall refer to a technology solution to continuously monitor and update RCCA’s security posture while preventing, detecting, analyzing, and responding to Security Incidents.

2.9. “Division” or “Division of Consumer Affairs” shall refer to the New Jersey Division of Consumer Affairs.

2.10. “Electronic Protected Health Information” or “ePHI” shall be defined in accordance with 45 C.F.R. § 160.103.

2.11. “July Incident” shall refer to the Security Incident, and all events related thereto, discovered by RCCA on July 25, 2019, in which RCCA improperly sent May Incident notification letters to patients’ correct mailing addresses, but containing a salutation line addressed to the prospective next-of-kin for 13,047 living individuals affected by May Incident.

2.12. “May Incident” shall refer to the Security Incident, and all events related thereto, discovered by RCCA on May 24, 2019, and publicly announced on July 23, 2019, in which an individual(s) gained unauthorized access to RCCA employee email accounts where PI, PHI and/or ePHI was stored, and which impacted approximately 105,200 individuals nationwide.

2.13. “Minimum Necessary Standard” shall refer to the requirements of the Privacy Rule that, when using or disclosing PHI or when requesting PHI from another Covered Entity or Business Associate, a Covered Entity or Business Associate must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request as defined in 45 C.F.R. § 164.502(b) and § 164.514(d)(1)-(5).

2.14. “Multi-factor Authentication” shall mean user account authentication through verification of at least two of the following factors: (i) knowledge factors such as a password; or (ii) possession factors, such as a token, connection through a known authenticated source, or a text

message on a mobile phone; or (iii) inherent factors, such as biometric characteristics.

2.15. “New Jersey” or “State” shall refer to the State of New Jersey.

2.16. “Personal Information” or “PI” shall mean the data elements in the definition of personal information set forth in the Identity Theft Protection Act, N.J.S.A. 56:8-161 to -166.3.

2.17. “Privacy Rule” shall refer to 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E.

2.18. “Protected Health Information” or “PHI” shall be defined in accordance with 45 C.F.R. § 106.103.

2.19. “RCCA MD” shall mean RCCA MD LLC, its wholly owned, integrated, and operated affiliates, subsidiaries, and divisions, successors, and assigns, directors and officers, and employees doing business in the United States.

2.20. “RCCA MSO” shall mean RCCA MSO LLC, its wholly owned, integrated, and operated affiliates, subsidiaries, and divisions, successors, and assigns, directors and officers, and employees doing business in the United States.

2.21. “RCCA Network” shall mean the networking equipment, databases or data stores, applications, servers, workstations, and endpoints owned and/or operated by RCCA, which are capable of using and sharing software, data, and hardware resources.

2.22. “Regional Care” shall mean Regional Cancer Care Associates LLC, its wholly owned, integrated, and operated affiliates, subsidiaries, and divisions, successors, and assigns, directors and officers, and employees doing business in the United States.

2.23. “Security Incident” shall be defined in accordance with 45 C.F.R. § 106.103.

2.24. “Security Information and Event Management” and “SIEM” shall mean software

and/or services that carry out analysis of event and log data in real-time to provide event correlation, threat monitoring, and incident response, as well as retrieve and analyze log data and generate a report.

2.25. “Security Rule” shall refer to 45 C.F.R Part 160 and 45 C.F.R Part 164, Subparts A and C.

3. STIPULATED FACTS

3.1. RCCA is comprised of privately owned, limited liability corporations all incorporated in New Jersey and headquartered at 25 Main St., Hackensack, New Jersey.

3.2. RCCA offers cancer treatment and related services across 30 locations in New Jersey, Maryland, and Connecticut.

3.3. RCCA MSO is the management services entity for Regional Care and RCCA MD.

3.4. At all relevant times, RCCA was and continues to be a Covered Entity within the meaning of HIPAA.

3.5. As a Covered Entity, RCCA is required to comply with the standards set forth by HIPAA that govern the privacy of PHI, including the Privacy Rule, Security Rule, and Breach Notification Rule.

3.6. In or around January of 2019, RCCA began alerting its employees to the increase in phishing attacks directed to the RCCA Network.

3.7. On January 9, 2019, RCCA sent its employees an email with the subject title “Unusual High Phishing Activity - Be Alert!”. The email warned RCCA employees about phishing emails, briefly identified ways to spot them, and advised employees to be alert to such emails.

3.8. On April 4, 2019, RCCA sent a second email to employees again warning that RCCA was receiving a high number of phishing emails. The email advised employees that RCCA would implement Barracuda Email Security Service (“Barracuda”) to filter all emails.

3.9. Neither the email sent on January 9, 2019, nor on April 4, 2019, included any process to verify that employees had received and reviewed them. RCCA is unable to produce any other form of training to prevent unauthorized access through phishing attacks prior to the May Incident.

3.10. Prior to May Incident, in 2017, 2018, and 2019, Atlantic performed annual cybersecurity risk assessments and prepared work plans on RCCA’s behalf, but these assessments and work plans failed to conduct any analysis regarding the prevention of phishing attacks.

3.11. Just prior to May Incident, on or around April 10, 2019, Barracuda technology was installed on all RCCA email accounts.

3.12. Despite the installation of Barracuda, between April 17, 2019, and June 4, 2019, RCCA employee email accounts were subject to unauthorized access.

3.13. On or around April 17, 2019, an unauthorized actor accessed an RCCA employee email account through a phishing attack. The initial phishing email instructed employees to click on a link to cancel a purported Microsoft Office 365 account deactivation. An RCCA employee clicked on the link and subsequently provided the unauthorized actor with the credentials for the employee’s RCCA email account.

3.14. After the unauthorized actor received the initial employee’s credentials, the unauthorized actor logged onto the compromised employee’s email account via a web portal and sent additional phishing emails from that compromised account to other RCCA employees.

3.15. On May 14, 2019, the unauthorized actor, using the compromised account, sent a phishing email to RCCA employees requesting that they complete a survey required by RCCA’s

CEO. To complete the survey, RCCA employees were required to provide the credentials for their RCCA email account. Eleven RCCA employees provided their account credentials in response to the phishing attack, compromising 11 RCCA employee email accounts.

3.16. Prior to and at the time of the May Incident, RCCA did not implement multi-factor authentication.

3.17. On May 24, 2019, an RCCA Human Resources Payroll Administrator received email communications claiming to be from two separate RCCA MSO employees, both requesting changes to their direct deposit banking information. In response, the Payroll Administrator notified RCCA's managed IT services vendor, Atlantic, because the requested changes went against RCCA's internal Payroll Policies. Atlantic thereafter began investigating the issue.

3.18. On or around May 27, 2019, Atlantic confirmed that the suspicious emails came from internal compromised RCCA employee email accounts.

3.19. On or around June 3, 2019, RCCA's outside legal counsel retained a third-party forensic investigative firm to conduct a forensic investigation to confirm the full scope of May Incident. The third-party investigative firm discovered that a total of 12 RCCA email accounts had been compromised through a targeted phishing scheme that allowed access to ePHI and PI stored on those email accounts.

3.20. RCCA's investigation confirmed that the PI and ePHI of 105,200 individuals were accessible to the unauthorized actor through the 12 RCCA email accounts compromised by the May Incident.

3.21. The 12 compromised RCCA email accounts contained ePHI of patients in RCCA LLC's and RCCA MD's oncology/hematology medical practice, generated for a variety of patient care purposes. This ePHI included, but was not limited to, communications regarding patient

appointments, handling of patient billing accounts, insurance matters, patient testing results, and patient identifying spreadsheets used for private payor reimbursement programs.

3.22. The 12 compromised RCCA email accounts also contained a limited amount of PI of RCCA patients, including, but not limited to driver's licenses, state issued identification numbers, social security numbers, financial account numbers, and payment card information.

3.23. RCCA did not utilize a Security Information and Event Management Program at the time of May Incident.

3.24. Due to limited logging capabilities in RCCA's email software platform, RCCA was unable to determine the specific consumer information compromised by May Incident.

3.25. RCCA notified the New Jersey Division of State Police and the population affected by May Incident on July 23, 2019.

3.26. On July 25, 2019, RCCA learned that 13,047 living individuals' May Incident notification letters were erroneously addressed in the salutation line of the letter to those individuals' prospective next-of-kin.

3.27. On August 1, 2019, RCCA mailed supplemental notices to individuals affected by the July Incident.

3.28. RCCA sent supplemental notice to the New Jersey Division of State Police and the population affected by May Incident on August 30, 2019.

3.29. RCCA stipulates to the enumerated facts stated in Section 3 for purposes of this Consent Order only.

4. ALLEGED VIOLATIONS OF LAW

4.1. The Division has alleged the following:

4.1.1. At all relevant times set forth in Section 3 above (the “Relevant Time Period”), incorporated herein by reference, RCCA was and continues to be a Covered Entity.

4.1.2. During the Relevant Time Period, RCCA has offered for Sale and Sold services, which are Merchandise within the meaning of the CFA.

4.1.3. As a Covered Entity, RCCA was, and continues to be, required to comply with HIPAA standards governing the privacy and security of PHI and/or ePHI, including, but not limited to the Security Rule, the Privacy Rule, and the Breach Notification Rule.

4.1.4. RCCA violated the CFA, HIPAA’s Security Rule, and HIPAA’s Privacy Rule when it failed to employ reasonable administrative and technological safeguards to protect the confidentiality of PI and ePHI of 105,200 consumers.

4.1.5. RCCA violated the CFA, HIPAA’s Security Rule, HIPAA’s Privacy Rule, and HIPAA’s Breach Notification Rule when it failed to properly notify 13,047 consumers of May Incident, improperly disclosing their PHI to unauthorized individuals.

4.1.6. Specifically, RCCA failed to comply with HIPAA’s Security Rule, Privacy Rule and Breach Notification Rule by:

- Failing to ensure the confidentiality, integrity, and availability of the ePHI of individuals affected by May Incident in violation of 45 C.F.R. §164.306(a)(1);
- Failing to ensure the confidentiality, integrity, and availability of the ePHI of individuals affected by the July Incident in violation of 45 C.F.R. §164.306(a)(1);
- Failing to protect against reasonably anticipated threats or hazards to the security or integrity of ePHI in violation of 45 C.F.R. §164.306(a)(2);

- Failing to conduct an accurate and thorough risk assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI, and to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in violation of 45 C.F.R. §164.308(a)(1)(ii)(A);
- Failing to implement a security awareness and training program for all members of its workforce in violation of 45 C.F.R. §164.308(a)(5)(i);
- Failing to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a) in violation of 45 C.F.R. §164.308(a)(1)(ii)(B);
- Failing to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. §164.308(a)(1)(ii)(C);
- Failing to implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner, or document why implementation of such a mechanism was not reasonable or appropriate, and implement an equivalent alternative measure, in violation of 45 C.F.R. §164.312(c)(2);
- Failing to implement procedures to verify that the person seeking access to ePHI is who they claim to be in violation of 45 C.F.R. §164.312(d); and
- Failing to properly address salutations in notifications to 13,047 individuals within the 60 days following the discovery of May Incident in violation of 45 C.F.R. §164.400-41.

4.1.7. RCCA's failure to ensure the proper security of RCCA's Network, which led to the subjugation of 105,200 customers' ePHI and PI in May Incident to unauthorized access, constitutes separate and additional violations of the CFA, N.J.S.A. 56:8-2.

4.1.8. RCCA's failure to ensure the proper mailing of May Incident notification letters, which led to the July Incident exposure of 13,047 patients' PHI, constitutes separate and additional violations of the CFA, N.J.S.A. 56:8-2.

5. AGREED-UPON BUSINESS PRACTICES

A. Compliance with State and Federal Law

5.1. RCCA shall not engage in conduct in violation of the CFA, ITPA, and HIPAA, including the Privacy Rule, Security Rule, and/or Breach Notification Rule, in connection with the security, collection, use, disclosure, storage, or disposal of PI, PHI, or ePHI.

5.2. RCCA shall not misrepresent the extent to which it maintains and protects the privacy, security, or confidentiality of PI, PHI, or ePHI collected from or about consumers.

B. Information Security and Privacy Program

5.3. RCCA shall develop, implement, and maintain a written information security and privacy program ("Information Security Program") that is reasonably designed to protect the security, integrity, and confidentiality of PI and PHI that RCCA collects, stores, transmits, maintains, and/or destroys. The Information Security Program shall, at minimum, include the specific information requirements set forth in Paragraphs 5.4 through 5.29 of this Consent Order.

5.4. The Information Security Program shall comply with any applicable requirements under State or federal law, and shall contain administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of RCCA's operations; (ii) the nature and scope of RCCA's activities; and (iii) the sensitivity of the PI, PHI, and ePHI that RCCA collects, stores,

transmits and/or maintains.

5.5. The Information Security Program shall be written and modified to allow access to PHI and ePHI consistent with the Minimum Necessary Standard. RCCA shall consider and adopt where reasonably feasible the principles of “zero trust architecture” throughout the RCCA Network. As used herein, “zero trust architecture” means RCCA will:

- i. Regularly monitor, log, and inspect network traffic, including log-in attempts, through the implementation of hardware, software, or procedural mechanisms that record and evaluate such activity;
- ii. Authorize and authenticate relevant device, user, and network activity within the RCCA Network; and
- iii. Require appropriate authorization and authentication prior to any user’s access to the RCCA Network.

5.6. As part of its Information Security Program, RCCA shall develop, implement, and maintain a written incident response plan to prepare for and respond to Security Incidents. RCCA shall review this response plan annually, then revise and update this response plan, as necessary, to adapt to any material changes that affect the security of PI, PHI, and ePHI. Such a plan shall, at a minimum, identify and describe the following phases: (i) Preparation; (ii) Detection and Analysis; (iii) Containment; (iv) Notification and Coordination with Law Enforcement; (v) Eradication; (vi) Recovery; (vii) Consumer and Regulator Notification and Remediation; and (viii) Post-Incident Analysis. If a Security Incident does not trigger the Breach Notification Rule or the ITPA, RCCA shall create a report that includes a description of the Security Incident and RCCA’s response to that Security Incident (“Security Incident Report”). The Security Incident Report shall be maintained for a period of ten (10) years from the date of the Security Incident.

5.7. RCCA shall employ an executive or officer who shall be responsible for implementing, maintaining, and monitoring the Information Security and Privacy Program (“Chief Information Security Officer” or “CISO”). The CISO shall have the background and expertise in information security appropriate to: (i) the size and complexity of RCCA’s operations; (ii) the nature and scope of RCCA’s activities; and (iii) the sensitivity of the PI, PHI, and ePHI that RCCA collects, stores, transmits and/or maintains.

5.8. The Role of the CISO will include regular and direct reporting to RCCA’s Chief Executive Officer (“CEO”), HIPAA Privacy and Security Officer (“HPSO”), Executive Staff, and Board of Directors concerning RCCA’s security posture, the risks faced by RCCA, and the implications of RCCA’s business decisions. The CISO shall provide a tangible report to: (1) the Board of Directors on at least a semi-annual basis; and (2) the CEO and HPSO on at least a quarterly basis. Such reports shall indicate any Security Incidents during the relevant time period.

5.9. The Information Security Program shall be memorialized in writing, maintained by the HPSO, and represent to consumers RCCA’s most current Information Security Program appropriately and accurately. The CISO and HPSO shall review these policies at least annually. Any substantive changes to the policies shall be updated with a brief description of the changes and the date on which the changes were made. All substantive changes shall be tracked in a change log at the bottom of each document. If there are no changes made during a review process, the CISO and HPSO shall acknowledge that in the change logs at the bottom of each document.

5.10. RCCA shall review not less than annually the Information Security Program to ensure compliance with industry standards.

5.11. The CISO shall, in collaboration with the HPSO, report to RCCA’s CEO, Executive Staff, and Board of Directors within twenty-four (24) hours of a confirmed Security

Incident impacting any consumers residing in the United States.

5.12. Within thirty (30) days of the employment of the CISO, RCCA shall provide a statement, in writing to the Division that it has designated a CISO. This writing shall also include the name of the HPSO for RCCA and documentation of her, his, or their background and expertise.

5.13. RCCA shall provide notice of the requirements of this Consent Order to all RCCA employees and Business Associates. RCCA shall implement trainings required to comply with the Information Security Program to all employees within ninety (90) days of the Effective Date of this Consent Order.

5.14. RCCA shall ensure that its Information Security Program receives the resources and support reasonably necessary to function as intended.

C. Specific Information Security Requirements

5.15. **Data Collection & Retention:** RCCA shall develop, implement, and maintain reasonable policies and procedures governing its collection, use, and retention of PI, PHI, and ePHI. RCCA shall limit its use, disclosure of, and requests for PHI and ePHI in accordance with the Minimum Necessary Standard, to fulfill all applicable State and federal regulatory, legal, and contractual obligations.

5.16. **Cyber Security Operations Center (“C-SOC”):** RCCA shall maintain the existence and operation of a C-SOC or a reasonably equivalent technology. The C-SOC shall provide comprehensive monitoring of servers and other technologies, including those related to electronic mail, to identify improper use of data, including PI, PHI, and/or ePHI. The C-SOC’s analytic capabilities shall be deployed to detect, analyze, and respond to potential and confirmed Security Incidents. The C-SOC shall identify the areas in which RCCA is transmitting and storing PI, PHI and ePHI, and operatively ensure that RCCA is using best practices to protect PI, PHI and

ePHI.

5.17. **Logging & Monitoring:** RCCA shall develop, implement, and maintain reasonable policies and procedures designed to properly log and monitor the RCCA Network and Covered Systems that collect, process, transmit, and/or store PI, PHI, and/or ePHI, in accordance with HIPAA. In furtherance of these policies and procedures, at minimum:

- a. RCCA shall employ tools such as a Security Information and Event Monitoring solution or a reasonably equivalent technology (“SIEM”), to log and monitor network traffic to detect and respond to Security Incidents.
- b. RCCA shall take reasonable steps to ensure the SIEM used pursuant to subsection (a) is properly configured, and regularly updated or maintained, and shall take reasonable steps to adequately log system activity and identify potential Security Incidents for review. Using the SIEM, RCCA shall actively review and analyze in real-time the logs of system activity and take appropriate follow-up actions with respect to Security Incidents. RCCA shall create a formalized procedure to track Security Incidents and alerts, and RCCA’s response, on a regular basis.
- c. RCCA shall maintain logs of system activity in conformance with industry standards and all applicable State and federal laws.
- d. RCCA’s CISO and HPSO shall implement and maintain these policies and procedures. The CISO and HPSO shall review these policies and procedures at least annually. Any substantive changes to the policies and procedures shall be updated with a brief description of the changes and the date on which the changes were made. All substantive changes shall be tracked in a change log at the bottom of each document. If there are no changes made during a review process, the CISO and HPSO

shall acknowledge that in the change logs at the bottom of each document.

- e. Any logging and monitoring conducted pursuant to this paragraph shall be coordinated by the CISO and performed by appropriately trained and experienced personnel.

5.18. **Email Filtering and Phishing Solutions:** RCCA shall maintain email protection and filtering solutions for all RCCA's email accounts, including the filtering of unsolicited bulk emails, and protections from phishing attacks, and other email malware attacks.

5.19. **Access Controls:** RCCA shall implement and maintain appropriate controls to manage access to and use of all accounts that can access PI, PHI, or ePHI, including individual accounts, administrator accounts, service accounts, and vendor accounts. Such controls shall include a means to regularly review access and access levels of users and remove network and remote access at the time of notification of termination for any employee whose employment has ended or any non-associate whose term has ended, in accordance with HIPAA.

5.20. **Authentication:** RCCA shall implement and maintain reasonable policies and procedures requiring the use of authentication in accordance with industry standards, including as appropriate under industry standards, strong passwords, password rotation, multi-factor authentication, and ensuring that stored passwords are protected from unauthorized access.

5.21. **Asset Inventory:** RCCA shall develop, maintain, and regularly update a reasonable inventory of the assets that primarily comprise the RCCA Network and appropriately identify and secure assets containing PHI and ePHI.

5.22. **Data Loss/Exfiltration Prevention:** RCCA shall develop, implement, and maintain a data loss prevention technology or a reasonably equivalent technology to detect and prevent unauthorized data exfiltration from the RCCA Network.

5.23. **Risk Assessments:** RCCA shall develop, implement, and maintain a risk

assessment program to identify, address, and as appropriate, remediate risks affecting its Covered Systems. At a minimum, RCCA shall have an annual risk assessment performed by an independent third party. The assessment shall identify all the areas where RCCA stores PI, PHI, and ePHI, and include assessment of all reasonably anticipated, internal, and external risks to the security, confidentiality, or availability of PI, PHI, and ePHI collected, processed, transmitted, stored, or disposed of by RCCA. Such reports shall be maintained by the CISO and the HPSO and made available for inspection by the Third-Party Assessor described in paragraph 5.26 of this Consent Order, and a copy of the report shall be produced to the Division within ten (10) days of completion for a total period of five (5) years.

5.24. **Employee Training:** RCCA shall conduct an initial training for all new employees no later than thirty (30) days after their employment and, on at least an annual basis, train existing employees concerning its information privacy and security policies, the proper handling and protection of PI, PHI, and ePHI, and disciplinary measures for violation, up to and including termination. RCCA must further document its employee trainings and include that in its annual risk analysis.

D. Information Security Program Assessment

5.25. RCCA shall obtain an information security assessment of its policies and practices pertaining to the collection, storage, maintenance, transmission, and disposal of PI and PHI, from an independent third-party professional (“Third-Party Assessor”) within one hundred twenty (120) days of the Effective Date of this Consent Order and then once a year thereafter for a term of five (5) years.

5.26. The Third-Party Assessor must be an organization that employs at least one individual to perform the assessment that is: (a) qualified as a Certified Information System

Security Professional (“CISSP”) or as a Certified Information Systems Auditor (“CISA”), or a similar qualification; and (b) has at least five (5) years of experience evaluating the effectiveness of computer systems and information system security.

5.27. Each year, the Third-Party Assessor shall at minimum review this Consent Order, the most recent Security Incident Report and recent internal risk assessments provided by RCCA as set forth in Paragraphs 5.6 and 5.23 respectively. The Third-Party Assessor shall prepare a formal (“Security Report”) that shall confirm RCCA’s development, implementation, and maintenance of a written Information Security Program with security controls and processes that meet the requirements of this Consent Order related to: access controls, including privileged access management and Multi-factor Authentication, vulnerability scanning and remediation, logging and monitoring, email filtering, and information system activity review and detection. The Security Report shall also confirm that RCCA has complied with the provisions of this Consent Order related to the employment of a CISO, maintenance of a CSOC facility, and information security training.

5.28. RCCA shall provide the initial Security Report to the Division no later than one hundred eighty (180) days after the Effective Date, and shall submit each subsequent Security Report to the Division no later than ten (10) days after its completion. RCCA will also provide the risk assessment, as set forth in Paragraph 5.23, to the New Jersey Attorney General on an annual basis during the five-year term.

5.29. Upon receipt of each Security Report, RCCA shall review and evaluate whether to revise its current policies and procedures based on the findings of the Security Report. Within sixty (60) days of RCCA’s receipt of each Security Report, RCCA shall make available to the Division a written description of any action it plans to take, or if no action is taken, a detailed

description why no action is necessary, in response to each Security Report.

5.30. Following the five-year terms specified in Paragraphs 5.23, 5.25, and 5.27, RCCA shall continue to conduct risk assessments and information security assessments on an annual basis for the following five (5) years, as required by HIPAA and as determined by the HPSO and CISO, which are to be memorialized in written reports. The Division reserves the right to request copies of reports from any information security assessments and risk assessments conducted by RCCA for five (5) years following the five-year terms specified in Paragraphs 5.23, 5.25, and 5.27.

5.31. The Division, shall, to the extent permitted by State law, treat all documents produced pursuant to Paragraphs 5.28, 5.29, and 5.30 as exempt from disclosure as applicable under the New Jersey Open Public Records Act, N.J.S.A. 47:1A-1 to -13. In lieu of providing electronic copies of documents specified in Paragraphs 5.28, 5.29, and 5.30 for retention by the Division, RCCA may establish a virtual viewing environment to satisfy its obligations pursuant to these Paragraphs.

6. SETTLEMENT PAYMENT

6.1. The Parties have agreed to a settlement of the Investigation in the amount of \$425,000 (“Settlement Payment”). This Settlement Payment consists of \$353,820 allocated to the Division’s civil penalty claims, and \$71,180.00 allocated to the Division’s claims for reimbursement of attorneys’ fees and investigative costs. The allocation of the Settlement Payment is not a finding or admission by RCCA of liability.

6.2. RCCA shall remit the Settlement Payment to the Division within forty-five (45) days after the Effective Date.

6.3. RCCA shall make the Settlement Payment by wire transfer, credit card, or by certified check, cashier’s check or money order made payable to the “New Jersey Division of

Consumer Affairs” and forwarded to:

Case Initiation and Tracking Unit
New Jersey Department of Law and Public Safety
Division of Consumer Affairs
124 Halsey Street – 7th Floor
P.O. Box 45025
Newark, New Jersey 07101
Attention: Van Mallett, Lead Investigator

6.4. Upon making the Settlement Payment, RCCA shall immediately be fully divested of any interest in, or ownership of, the money paid. All interest in the Settlement Payment, and any subsequent interest or income derived therefrom, shall inure entirely to the benefit of the Division pursuant to the terms herein.

7. GENERAL PROVISIONS

7.1. This Consent Order is entered into by the Parties as their own free and voluntary act and with full knowledge and understanding of the obligations and duties imposed by this Consent Order.

7.2. This Consent Order shall be governed by, and construed and enforced in accordance with, the laws of the State of New Jersey.

7.3. The Parties have negotiated, jointly drafted, and fully reviewed the terms of this Consent Order and the rule that uncertainty or ambiguity is to be construed against the drafter shall not apply to the construction or interpretation of this Consent Order.

7.4. This Consent Order contains the entire agreement among the Parties. Except as otherwise provided herein, this Consent Order shall be modified only by a written instrument signed by or on behalf of the Parties.

7.5. Except as otherwise explicitly provided in this Consent Order, nothing herein shall be construed to limit the authority of the Attorney General to protect the interests of the State or

the people of the State.

7.6. If any portion of this Consent Order is held invalid or unenforceable by operation of law, the remaining terms of this Consent Order shall not be affected.

7.7. This Consent Order shall be binding upon the Parties and their successors in interest. In no event shall assignment of any right, power, or authority under this Consent Order avoid compliance with this Consent Order.

7.8. This Consent Order is entered into by the Parties for settlement purposes only. Neither the fact of nor any provision contained in this Consent Order shall constitute or be construed as: (a) an approval, sanction, or authorization by the Attorney General, the Division, or any other governmental unit of the State of any act or practice of RCCA; or (b) an admission by RCCA that it violated the CFA, ITPA, or HIPAA, including the Privacy Rule, Breach Notification Rule, and/or the Security Rule, or any other federal or State law, administrative rule or regulation, or an express or implied admission of any other matter of fact or law, or of any liability or wrongdoing.

7.9. This Consent Order is not intended, and shall not be deemed, to constitute evidence or precedent of any kind in any action or proceeding except in an action or proceeding: (a) by one of the Parties to enforce, rescind, or otherwise implement any or all of the terms herein; or (b) involving a Released Claim (as defined in Section 8) to support a defense of res judicata, collateral estoppel, release, or other theory of claim preclusion, issue preclusion, or similar defense.

7.10. The Parties represent and warrant that their signatories to this Consent Order have authority to act for and bind the respective Party.

7.11. Unless otherwise prohibited by law, any signatures by the Parties required for filing of this Consent Order may be executed in counterparts, each of which shall be deemed an original,

but all of which shall constitute one and the same Consent Order. Electronic signatures shall constitute acceptable, binding signatures for purposes of this Consent Order.

8. RELEASE

8.1. In consideration of the undertakings, mutual promises, and obligations provided for in this Consent Order and conditioned on RCCA making the Settlement Payment as described in Section 6, the Division hereby agrees to release RCCA from any and all civil claims or causes of action, or consumer-related administrative claims or actions, to the extent permitted by law, which the Division could have brought prior to the Effective Date against RCCA for violations of any consumer protection law administered or enforced by the Division, CFA, ITPA, or HIPAA, including the Privacy Rule, Breach Notification Rule, and/or Security Rule, arising out of the Investigation, as well as the matters specifically addressed in this Consent Order (“Released Claims”).

8.2. Notwithstanding any term of this Consent Order, the following do not comprise Released Claims: (a) private rights of action; (b) actions to enforce this Consent Order; and (c) any claims against RCCA by any other agency or subdivision of the State except any civil claims or causes of action, or consumer-related administrative claims or actions, arising out of the Investigation as well as the matters specifically addressed in this Consent Order that the Division could have brought but has released in Section 8.1 above.

9. PENALTIES FOR FAILURE TO COMPLY

9.1. The Attorney General (or designated representative) shall have the authority to enforce the provisions of this Consent Order or to seek sanctions for violations hereof or both.

9.2. Prior to filing any action to enforce the provisions of this Consent Order, the Attorney General (or designated representative) shall meet and confer with RCCA in an attempt

to resolve any dispute with respect to compliance with this Consent Order. The Attorney General (or designated representative) shall notify RCCA in writing of the alleged violation of this Consent Order, and RCCA shall have fifteen (15) days to respond to the notification. The Attorney General (or designated representative) shall not file any action until such 15-day time period to respond has expired.

10. COMPLIANCE WITH ALL LAWS

10.1. Except as provided in this Consent Order, no provision herein shall be construed as:

- a. Relieving RCCA of its obligations to comply with all State and federal laws, regulations, or rules, as now constituted or as may hereafter be amended; granting permission to engage in any acts or practices prohibited by any such laws, regulations, or rules; or requiring RCCA to take an action that is prohibited by such laws, regulations, or rules; or
- b. Limiting or expanding any right the Division may otherwise have to obtain information, documents, or testimony from RCCA pursuant to any State or federal law, regulation, or rule, as now constituted or as may hereafter be amended, or limiting or expanding any right RCCA may otherwise have pursuant to any State or federal law, regulation, or rule, to oppose any process employed by the Division to obtain such information, documents, or testimony.

11. NOTICE

11.1. Except as otherwise provided herein, any notices or other documents required to be sent to the Division or RCCA pursuant to this Consent Order shall be sent by United States mail, Certified Mail Return Receipt Requested, or other nationally recognized courier service that provides for tracking services and identification of the person signing for the documents and simultaneously by electronic mail. The notices and/or documents shall be sent to the following addresses:

For the Division:

Kashif T. Chand, Deputy Attorney General
Office of the Attorney General
Department of Law and Public Safety
124 Halsey Street, 5th Floor
Newark, New Jersey 07101
Kashif.Chand@law.njoag.gov


For RCCA:

Regional Cancer Care Associates
25 Main Street, Ste. 601
Hackensack, New Jersey 07601

Attn: Legal Department

IT IS ON THE 15th DAY OF December, 2021 SO ORDERED.

ANDREW J. BRUCK
ACTING ATTORNEY GENERAL OF NEW JERSEY

By: 
SEAN P. NEAFSEY, ACTING DIRECTOR
DIVISION OF CONSUMER AFFAIRS

THE PARTIES CONSENT TO THE FORM, CONTENT AND ENTRY OF THIS CONSENT ORDER ON THE DATES ADJACENT TO THEIR RESPECTIVE SIGNATURES.

FOR THE DIVISION:

ANDREW J. BRUCK
ACTING ATTORNEY GENERAL OF NEW JERSEY

By: _____

Gina F. Pittore
Deputy Attorney General
124 Halsey Street, 5th Floor
Newark, New Jersey 07101

Dated: _____, 2021

FOR RCCA MSO LLC:

By: _____

Terrill Jordan
President & CEO

Dated: 12.9 _____, 2021

FOR Regional Cancer Care Associates LLC:

By: _____

Terrill Jordan
President & CEO

Dated: 12.9 _____, 2021

FOR RCCA MD LLC:

By: _____


Terrill Jordan
President & CEO

Dated: 12.9 _____, 2021

THE PARTIES CONSENT TO THE FORM, CONTENT AND ENTRY OF THIS CONSENT ORDER ON THE DATES ADJACENT TO THEIR RESPECTIVE SIGNATURES.

FOR THE DIVISION:

ANDREW J. BRUCK
ACTING ATTORNEY GENERAL OF NEW JERSEY

By: 

Gina F. Pittore
Deputy Attorney General
124 Halsey Street, 5th Floor
Newark, New Jersey 07101

Dated: December 9, 2021

FOR RCCA MSO LLC:

By: _____

Terrill Jordan
President & CEO

Dated: _____, 2021

FOR Regional Cancer Care Associates LLC:

By: _____

Terrill Jordan
President & CEO

Dated: _____, 2021

FOR RCCA MD LLC:

By: _____

Terrill Jordan
President & CEO

Dated: _____, 2021