STATE OF COLORADO
DEPARTMENT OF LAW

ASSURANCE OF DISCONTINUANCE

IN THE MATTER OF BROOMFIELD SKILLED NURSING AND REHABILITATION CENTER, LLC

This Assurance of Discontinuance ("Assurance") is entered into between the State of Colorado, *ex rel.* Philip J. Weiser, Attorney General for the State of Colorado ("Attorney General" or "State"), and Broomfield Skilled Nursing and Rehabilitation Center ("Broomfield") pursuant to the Attorney General's powers under Colo. Rev. Stat. Section 6-1-110(2) and constitutes a complete settlement between the State and Broomfield (the "Parties") regarding the State's allegations as to the security breach that Broomfield first detected on March 3, 2021.

I. INTRODUCTION

A cybercriminal cannot steal data that is not there. Threats of cybercrime and identity theft are exacerbated by the overcollection, overuse, and over-retention of unnecessary personal information, which is then accessed by threat actors in the event of a data breach. It is crucial that companies offset those threats by practicing data minimization coupled with effective data disposal, limiting their collection and maintenance of personal information to that which is necessary for a specific data processing purpose. Colorado law underscores the importance of those principles by

statutorily obligating companies to develop written policies for the destruction or proper disposal of documents that contain personally identifying information once those documents are no longer needed.

Broomfield did not maintain a data disposal policy or otherwise fully comply with the data security safeguards required by Colorado law, and failed to notify Colorado residents of its March, 2021, data breach in a timely manner. This Assurance addresses those violations of Colorado's data security and data breach notification laws.

II. PARTIES

1. Philip J. Weiser is the duly elected Attorney General for the State of Colorado and has express jurisdiction to investigate and prosecute violations of the Colorado Consumer Protection Act ("CCPA"), C.R.S. §§ 6-1-101 through 6-1-1121.

2. Broomfield is a Colorado corporation with a principal office address of 12975 Sheridan Blvd., Broomfield, Colorado 80020.

III. DEFINITIONS

3. The term "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and subsequent amendments and regulations.

4. The terms "Personal Identifying Information" and its abbreviation, "PII," mean the items set forth in C.R.S. Sections 6-1-713(1)(b) and 6-1-716(1)(g).

5. The term "Effective Date" means the first date upon which both Parties have executed and delivered this Assurance.

6. Unless otherwise specified, all definitions found in C.R.S. §§ 6-1-105(1), 6-1-713(2), and 6-1-716(1) are incorporated herein, and any term defined in those sections shall have the same meaning when used in this Assurance.

IV. STATE'S ALLEGATIONS

A. Colorado's Data Security Laws.

7. C.R.S. § 6-1-713 requires companies that maintain, own, or license paper or electronic documents containing PII to develop a written policy for the destruction or proper disposal of those paper and electronic documents when they are no longer needed.

8. C.R.S. § 6-1-713.5 requires companies that maintain, own, or license PII of Colorado residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the PII and the nature and size of the business and its operations.

9. Under C.R.S. 6-1-713.5(4), "A covered entity that is regulated by state or federal law and that maintains procedures for protection of personal identifying information pursuant to the laws, rules, regulations, guidances, or guidelines established by its state or federal regulator is in compliance" with C.R.S. § 6-1-713.5.

10. C.R.S. § 6-1-716 imposes obligations on companies that experience security breaches or potential security breaches. When a company becomes aware that a security breach may have occurred, the company must "conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused." *Id.* § 6-1-716(2). If the company determines that a data breach occurred, the company "shall give notice to the affected Colorado residents unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur." *Id.* The company must give notice to residents in "the most expedient time possible, but no later than thirty days after the date of determination that a security breach occurred." *Id.*

11. Under C.R.S. § 6-1-716(c), "[d]etermination that a security breach occurred" means "the point in time at which there is sufficient evidence to conclude that a security breach has taken place."

12. Under C.R.S. § 6-1-716(h), "Security breach" means "the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity."

B. Factual Allegations

13. On March 3, 2021, Broomfield learned that forwarding rules had been created in two employee email accounts. Broomfield hired a third-party forensic investigator, which completed an investigation in April, 2021. The forensic

investigator determined that the forwarding rules had been created by an unknown third party who gained access to the employee email accounts on March 2, 2021 by acquiring the employees' login credentials. The unknown party established an IMAP/POP connection with the employees' email accounts, giving the unknown party access to the employees' entire email inboxes.

14. At the time of the breach, twenty-seven of Broomfield's approximately thirty employee email accounts were equipped with two-party authentication. However, three workstations, including the two that were breached, were not equipped with 2-factor authentication.

15. At the time of the breach, all Broomfield staff Office 365 mailboxes were being transitioned to 2-factor authentication for access and the two affected email accounts were in the process of but did not yet have the 2-factor authentication enabled.

16. The breached employee inboxes contained PII of Colorado residents, including financial account information, Social Security numbers (SSNs), and driver license / state ID numbers. The breached employee inboxes also contained medical information of Coloradans who were residents of the facility. The accounts contained this PII in combination with the Colorado residents' first and last name or first initial and last name.

17. The PII of 677 Colorado residents was breached in the attack. Of these, 221 were current or former residents of the facility and 456 were current or former employees of the facility.

18. At the time of the breach, one of the two breached email accounts contained 42,530 emails and the other contained 33,573 emails.

19. One account had emails containing PII from as early as September 2016; the other had emails containing PII from as early as October 2017.

20. Broomfield maintained some systemwide data security safeguards at the time of the breach, which included:

- Maintaining Servers and Network Storage in a locked, air conditioned office;
- Using Microsoft Active Directory and AD DNS on its workstations;
- Maintaining an updated Business Class Firewall (Security Suite) and Managed Network devices (Virtual LANs);
- Running a business class Anti-Virus client;
- Maintaining group policies that include password expiration every 90 days, password complexity and password history requirements, and idle timeout locks on workstations;
- Purchasing the Point Click Care Charting system;

- Having Broomfield Census report to internal users sent to network folders rather than email;
- Encrypting local backups;
- Including security information and acceptable use requirements in the Employee Manual, and requiring new hires to sign and acknowledge the Employee Manual;

- For internal emails, Broomfield utilized a closed secure system of email which is not accessible to outside users;
- Broomfield required emails containing PII/PHI to be encrypted before sending to users outside the company;
    - User accounts were disabled when an employee left and Office 365 accounts removed to a Shared Mailbox that does not provide direct login access.

21. Broomfield was in the process of transitioning all employee Office 365 mailboxes to 2-factor authentication for access and all except three (3) of out of approximately thirty (30) Office 365 mailboxes had been transitioned at the time of the breach. Broomfield has since completed its implementation of 2-factor authentication on all remaining email accounts.

22. Broomfield learned of the security incident on March 3, 2021 when it was notified that two (2) employees had forwarding rules in their email accounts.

23. Starting June 2, 2021, Broomfield had a vendor manually review the documents contained in the two compromised accounts to determine whether they contained PII of Colorado residents. On June 25, 2021, the vendor completed the manual document review process. At that point, Broomfield had enough evidence to determine that the compromised email accounts contained PII of Colorado residents.

C. **Legal Allegations.**

24. The Attorney General's legal allegations are stated below. Broomfield does not admit and expressly disputes the Attorney General's allegations. Broomfield does not admit and expressly disputes the Findings set forth in Paragraphs 25 through 41 below, and does not admit to any violation of or liability arising from any federal, state, or local laws in stipulating to the entry of this Assurance.

a. Broomfield failed to comply with Colorado's data disposal statutes.

25. Under C.R.S. § 6-1-713, Broomfield was required to maintain a policy for the destruction or proper disposal of documents containing PII when such documents were no longer needed.

26. Broomfield violated C.R.S. § 6-1-713 by not maintaining a written policy for the destruction or proper disposal of documents containing PII when such documents were no longer needed.

b. Broomfield failed to comply with Colorado's data protection statutes.

27. Under C.R.S. § 6-1-713.5, Broomfield was required to implement reasonable security procedures and practices appropriate to the nature of the PII it maintained and the nature and size of Broomfield's business and its operations.

28. Broomfield is a skilled nursing facility with approximately two-hundred beds and hundreds of employees. By the nature of its business, Broomfield collects and maintains highly sensitive PII about Colorado residents.

29. Broomfield's practices and procedures did not prohibit or prevent its employees from collecting and storing highly sensitive PII in their employee email accounts, which created a risk that Broomfield was obligated to remedy through the application of appropriate safeguards.

30. As noted above, Broomfield maintained some systemwide data security safeguards (*see* Paragraph 20, *supra*). However, at the time of the breach Broomfield did not apply appropriate safeguards to at least the two compromised employee email accounts, each of which contained over 30,000 emails.

31. Reasonable safeguards for email accounts containing significant amounts of PII would include mechanisms such as 2-factor authentication, email encryption, and implementation of policies intended to limit the amount of PII contained in the email accounts. In the alternative, Broomfield could have collected PII through secure file-sharing software or by other, more secure means.

32. Under these circumstances, Broomfield failed to meet the reasonableness standard of C.R.S. § 6-1-713.5 by failing to apply appropriate safeguards to protect employee email accounts containing significant amounts of PII.

33. To the extent that Broomfield and the PII at issue is regulated by HIPAA, Broomfield still failed to meet the data security standards set forth in C.R.S. § 6-1-713.5. Under HIPAA, a covered entity must "Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits." The U.S. Department of Health and Human Services has advised that "while the Privacy Rule does not prohibit the use of unencrypted e-mail for treatment-related communications between health care providers and patients, other safeguards should be applied to reasonably protect privacy, such as limiting the amount or type of information disclosed through the unencrypted e-mail." Here, Broomfield did not encrypt the PII or PHI present in the breached email accounts, it had not implemented multifactor authentication on those accounts, it did not enforce a reasonable email disposal policy, no steps were taken to ensure the limitation of the amount or type of PHI in those accounts, and it maintained no policy requiring disposal of PHI in email accounts. Broomfield lacked appropriate PHI safeguards under HIPAA's security requirements, and therefore did not comply with C.R.S. § 6-1-713.5 as a HIPAA-covered entity.

34. Accordingly, Broomfield was not in compliance with C.R.S. § 6-1-713.5.

c. Broomfield failed to timely notify impacted Colorado residents.

35. Broomfield maintained, licensed, and/or owned PII of former and current residents and employees of Broomfield. Broomfield maintained the PII in combination with the residents' first and last name or first initial and last name.

36. When there was sufficient evidence to conclude that a security breach had taken place, Broomfield was required to provide notice to the impacted Coloradans within thirty days. See C.R.S. § 6-1-716(2)(A).

37. By March 2021, and at the latest, April 2021, Broomfield knew that malicious actors had compromised the email accounts and set forwarding rules.

38. By June 25, 2021, Broomfield had sufficient evidence to conclude that compromised email accounts contained PII of Colorado residents and that a security breach had therefore occurred.

39. Broomfield notified the affected Colorado residents on November 3, 2021, over four months after obtaining sufficient evidence to conclude that a breach had occurred.

40. This delay violated C.R.S. § 6-1-716.

41. The Attorney General believes that Broomfield's alleged violations of C.R.S. §§ 6-1-713, 6-1-713.5, and 6-1-716, as stated above, constituted a deceptive trade practice under the CCPA. C.R.S. § 6-1-105(1)(x).

V. LEGAL AUTHORITY

42. C.R.S. § 6-1-110(2) authorizes the Attorney General to accept an assurance of discontinuance of any deceptive trade practice listed in Part 7 of the CCPA. Section 6-1-110(2) also allows the Attorney General to accept a voluntary payment from Broomfield of the costs of the State's investigation and any action or proceeding by the Attorney General.

VI. CONSIDERATION

43. The Parties enter into this Assurance for the purpose of compromising and resolving all disputed claims and to avoid further expense of protracted litigation. This Assurance does not constitute an admission by Broomfield of any violation of the CCPA, nor shall it be construed as an abandonment by the State of its claim that Broomfield has violated the CCPA.

44. The Attorney General is assessing a fine on Broomfield in the amount of $60,000 to the State. Within 30 days of the Effective Date, Broomfield will pay $10,000 to the State. Within 60 days of the Effective Date, Broomfield will pay an additional $25,000 to the State. The State agrees to suspend Broomfield's payment of the remaining $25,000 if Broomfield complies fully with the terms outlined in paragraphs 45 - 53. Payment shall be in the form of a certified check, cashier's check, or money order made payable to the "Colorado Department of Law," shall reference

"In the Matter of Broomfield Skilled Nursing and Rehabilitation Center, LLC," and shall be delivered to:

Miriam Burnett, Administrative Assistant
Consumer Protection Section
Colorado Department of Law
1300 Broadway, 7th Floor
Denver, Colorado 80203

All payments under this paragraph 44 are to be held, along with any interest thereon, in trust by the Attorney General to be used in the Attorney General's sole discretion for reimbursement of the State's actual costs and attorneys' fees, the payment of restitution, if any, and for future consumer fraud or antitrust enforcement, consumer education, or public welfare purposes.

VII. FURTHER ASSURANCES OF BROOMFIELD

45. Broomfield, and any of its principals, officers, directors, agents, employees, representatives, successors, affiliates, subsidiaries, contractors, and assigns who have received actual notice of this Assurance, agree that:

A. Data Disposal Requirements.

46. Within 30 days of the Effective Date, Broomfield shall develop and implement a written policy for the destruction or proper disposal of paper and electronic documents containing PII that complies with C.R.S. § 6-1-713.

B. Information Security Requirements.

47. As part of Broomfield's compliance with this Assurance, within 90 days after the Effective Date, Broomfield shall update its existing written information security program (ISP) to include a data disposal policy.

48. Within 90 days after the Effective Date, Broomfield shall also review and update its existing ISP to ensure it is reasonably designed to protect the security, integrity, and confidentiality of PII, and contains administrative, technical, and physical safeguards appropriate to:

a. The size and complexity of Broomfield's operations;

b. The nature and scope of Broomfield's activities; and

c. The sensitivity of the PII that Broomfield maintains, licenses, or owns.

49. The ISP shall address the specific vulnerabilities leading to the breach, including:

a. Continuing to designate an employee to develop and implement the information security program;

b. Implementing an annual (at a minimum) security training and awareness program for all members of Broomfield's workforce on secure storage and handling of PII that includes but is not limited to phishing awareness and detection;

c. Documenting appropriate technical controls to secure PII with supporting rationale; and

d. Implementing policies and protocols for employee reporting of suspected or known security incidents and prompt institutional response.

50. Broomfield shall continue to, on at least an annual basis, review the safeguards it has put in place to protect PII to ensure proper implementation of the ISP and to ensure that Broomfield is up to date with any reasonably anticipated security threats.

C. Incident Response and Breach Notification Requirements.

51. Broomfield shall comply with the provisions of C.R.S. § 6-1-716 by creating an Incident Response Plan ("Plan") within 30 days after the Effective Date. The plan will include:

a. A designated employee responsible for developing and implementing the Plan;

b. Creation of an incident response team; and

c. A requirement that the incident response team establish milestones designating when the company will accomplish specific tasks to ensure that Broomfield complies with the requirements of C.R.S. § 6-1-716. On the date of each milestone, the company's incident response team must submit a written status report to Broomfield's leadership, including the president, detailing steps taken in the investigation to accomplish the given tasks.

52. Broomfield shall submit compliance reports, sworn under penalty of perjury by an individual or individuals with authority to bind Broomfield, to the Attorney General on the first and third anniversaries of the Effective Date of this Assurance. The compliance reports must:

a. Identify the primary postal and email address and telephone number, as designated points of contact, which the State may use

to communicate with Broomfield in connection with this Assurance;

b. Describe, in detail, the steps Broomfield has taken to comply with each paragraph of this Section VII;

c. Identify and describe all data security incidents or potential data security incidents that have occurred in the reporting period, including a detailed description of all steps taken in any investigations Broomfield has undertaken;

d. Describe all adjustments or improvements Broomfield has made as a result of any security incident or potential data security incident reported under paragraph 52(c), above;

e. Identify, describe and provide evidence of continued compliance with any security policy required or represented in this Assurance.

53. Broomfield further agrees to cooperate with any proceedings or investigations arising out of the State's monitoring or investigation of Broomfield's compliance with this Assurance. This includes submission of additional compliance reports the State may reasonably request, promptly responding to reasonable requests for information made by the State and accepting service of Civil Investigative Demands.

VIII. RELEASE

54. The State acknowledges by its execution hereof that this Assurance constitutes a complete settlement and release of all claims under the CCPA on behalf of the State against Broomfield with respect to all claims, causes of action, damages, fines, costs, and penalties which were asserted or could have been asserted under the CCPA for the conduct described in this Assurance, that arose prior to the Effective Date and relating to or based upon the acts or practices which are the subject of this Assurance. The State agrees that, except as provided in the following paragraph, it shall not proceed with or institute any civil action or proceeding under the CCPA against Broomfield for any conduct or practice prior to the Effective Date which relates to the subject matter of this Assurance.

55. Nothing herein precludes the State from enforcing this Assurance, or from pursuing any law enforcement action under the CCPA with respect to the acts or practices of Broomfield not covered by this Assurance or any acts or practices of Broomfield conducted after the Effective Date. Nothing herein shall be construed to be a waiver or limitation of Broomfield's legal rights, remedies, or defenses in connection with any claim, matter, or suit related to the subject matter of this Assurance other than an action by the State to enforce the provisions of this Assurance.

IX. ENFORCEMENT

56. The obligations set forth in this Assurance are continuing.

57. The Parties consent to venue and jurisdiction for any proceeding necessary to enforce the terms of this Assurance within the District Court, Broomfield County, Colorado.

58. A violation of any of the terms of this Assurance shall constitute a prima facie violation of the CCPA under C.R.S. § 6-1-110(2). If the State believes that Broomfield has violated any term of this Assurance, the State shall be entitled to file a civil action under the CCPA and to seek an injunction or other appropriate order from such court to enforce the provisions of this Assurance.

59. In any such action, upon a showing by the State of a material violation of this Assurance by Broomfield, Broomfield stipulates to 1) a judgment in the amount of $25,000, which reflects the suspended payment described in paragraph 44, above; and 2) an order converting this Assurance into a permanent injunction against Broomfield. The State may seek, and the Court may enter, any additional remedies, including but not limited to additional monetary remedies, that are deemed proper. Broomfield agrees to waive any counterclaims that it may have had with respect to the subject matter of this Assurance and agrees to limit any defenses to (1) whether a violation has occurred; (2) the remedies for the violation.

X. MISCELLANEOUS PROVISIONS

60. This Assurance is the final, complete, and exclusive statement of the Parties' agreement on the matters contained herein, and it supersedes, terminates, and replaces any and all previous negotiations, agreements, and instruments as may exist between the Parties. Other than any representation expressly stated in this Assurance, the Parties have not made any representations or warranties to each other, and no Party's decision to enter into this Assurance is based upon any statements by any other Party outside of those in this Assurance. No change or modification of this Assurance shall be valid unless in writing and signed by all Parties. If any provision(s) of this Assurance is held to be invalid, illegal, or unenforceable, the validity, legality, and enforceability of the remaining provisions shall not in any way be affected or impaired thereby.

61. This Assurance shall neither create nor waive or otherwise affect any private rights or remedies in any third parties nor waive any rights, remedies, or defenses of the Parties in respect to any third parties. Under no circumstances shall this Assurance or the name of the Attorney General or any of the State's employees or representatives be used by Broomfield or any person under their direction or control to suggest the State's endorsement of Broomfield's past, present, or future conduct.

62. Nothing herein relieves Broomfield of its duty to comply with all applicable laws, regulations, or rules of the State of Colorado nor constitutes

authorization by the State for Broomfield to engage in acts and practices prohibited by such laws.

63. Broomfield acknowledges that it is the State's customary position that an agreement restraining certain conduct by a party does not prevent the State from addressing later conduct that could have been prohibited, but was not, in the earlier agreement, unless the earlier agreement expressly limited the State's enforcement options in that manner. Therefore, nothing herein shall be interpreted to prevent the State from taking enforcement action to address conduct occurring after the Effective Date that the State believes to be in violation of the law. The fact that such conduct was not expressly prohibited by the terms of this Assurance shall not be a defense to any such enforcement action.

64. The terms and provisions of this Assurance may be enforced by the current Colorado Attorney General, and by any of his duly authorized agents or representatives, as well as by any of his successors in interest, and by any of his successors in interest's agents or representatives.

65. Pursuant to C.R.S. § 6-1-110(2), this Assurance shall be a matter of public record.

66. Broomfield acknowledges that it had a full opportunity to review this Assurance and consult with legal counsel regarding it. The undersigned representatives of Broomfield agree and represent that they have read and

understood this Assurance, accept the legal consequences involved in signing it, and that there are no other representations, agreements, or understandings between the State and Broomfield that are not stated in writing herein.

67. This Assurance may be signed in one or more counterparts, each of which shall be deemed an original, but which together shall constitute the Assurance. Electronic copies of this Assurance and the signatures hereto may be used with the same force and effect as an original.

XI. Notice

68. All notices regarding this Assurance shall be sent by certified mail, return receipt requested or reputable overnight delivery service (e.g., FedEx, UPS) at the addresses set forth below unless any Party notifies the other Parties in writing of another address to which notices should be provided:

If to Broomfield Skilled Nursing and Rehabilitation Center, LLC:

Aaron Mann
3G HealthCare | Principal
12995 Sheridan Boulevard
Suite 200
Broomfield, CO amann@3ghc.com

With copies to legal counsel by Regular U.S. Mail and e-mail:

Anjali C. Das
Wilson Elser Moskowitz Edelman & Dicker L.L.P.
55 West Monroe Street, Suite 3800
Chicago, IL 60603
Anjali.Das@WilsonElser.com

If to the State:

Colorado Attorney General
1300 Broadway, 7th Floor
Denver, Colorado 80203
Attn.: Abigail Hinchcliff, First Assistant Attorney General,
abigail.hinchcliff@coag.gov
Attn: Jill Szewczyk, Assistant Attorney General II, jill.szewczyk@coag.gov

[Signatures appear on the following page(s)]

STATE OF COLORADO:

PHILIP J. WEISER,
ATTORNEY GENERAL

By: _____

Jill Szewczyk
Assistant Attorney General II
Attorney Reg. No. 46902

BROOMFIELD SKILLED NURSING AND REHABILITATION CENTER, LLC

By: _____

Jonathan Dougherty
(Name of officer for BROOMFIELD)

_____

~~Anjali C. Das~~
Wilson Elser Jennifer Stegmaier

Attorney for Broomfield Skilled Nursing and Rehabilitation Center, LLC