

ENTERED
96

KEVIN JESPERSEN
ACTING ATTORNEY GENERAL OF NEW JERSEY
Division of Law
124 Halsey Street - 5th Floor
P.O. Box 45029
Newark, New Jersey 07101
Attorney for Plaintiffs

COPY

FILED

FEB 15 2007

SUP
MER
C

By: Elliott M. Siebers – ID# 033582012
Russell M. Smith, Jr. – ID# 014202012
Deputy Attorneys General
Brian McDonough – ID# 026121980
John M. Falzone – ID# 017192003
Assistant Attorneys General

SUPERIOR COURT OF NEW JERSEY
CHANCERY DIVISION, ESSEX COUNTY

DOCKET NO.: MER-C- 12 ~~17~~

KEVIN JESPERSEN, Acting Attorney
General of the State of New Jersey, and
STEVE C. LEE, Director of the New Jersey
Division of Consumer Affairs,

Plaintiffs,

v.

HORIZON HEALTHCARE SERVICES,
INC., d/b/a HORIZON BLUE CROSS BLUE
SHIELD OF NEW JERSEY,

Defendant.

FINAL CONSENT JUDGMENT

Plaintiffs Kevin Jespersen, Acting Attorney General of the State of New Jersey ("Attorney General") and Steve C. Lee, Director of the New Jersey Division of Consumer Affairs ("Director") (collectively, "Plaintiffs") have commenced this action by filing the Complaint herein;

COPY

WHEREAS the Attorney General is charged with the responsibility of enforcing the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 et seq. (“CFA”), and the Director 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 (“State” or “New Jersey”) and on behalf of the State in its sovereign capacity, may, pursuant to 42 U.S.C. § 1320d-5(d), enforce the provisions of 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 et seq. (collectively, “HIPAA”);

WHEREAS Plaintiffs alleged by Complaint that defendant Horizon Healthcare Services, Inc., d/b/a Horizon Blue Cross Blue Shield of New Jersey (“Horizon BCBSNJ”) engaged in conduct in violation of HIPAA and/or the CFA (“Complaint”);

WHEREAS Plaintiffs and Horizon BCBSNJ (collectively, “Parties”) have reached an amicable agreement hereby resolving the issues in controversy without the need for further action. As evidenced by their signatures below, the Parties do consent to the entry of this Consent Judgment and its provisions without trial or adjudication of any issue of fact or law, and without an admission of any liability or wrongdoing of any kind.

The Court has reviewed the terms of this Consent Judgment and based upon the Parties’ agreement and for good cause shown:

IT IS HEREBY ORDERED, ADJUDGED AND AGREED AS FOLLOWS:

JURISDICTION

1. The Parties admit jurisdiction of this Court over the subject matter and over the Parties for the purpose of entering into this Consent Judgment. The Court retains jurisdiction for the purpose of enabling the Parties to apply to the Court at any time for such further order and relief as may be necessary for the construction, modification, enforcement, execution or satisfaction of this Consent Judgment.

VENUE

2. Pursuant to N.J.S.A. 56:8-8, venue as to all matters between the Parties hereto relating to or arising out of this Consent Judgment shall lie exclusively in the Superior Court of New Jersey, Chancery Division, Mercer County.

EFFECTIVE DATE

3. This Consent Judgment shall be effective on the date it is entered by the Court ("Effective Date").

DEFINITIONS

As used in this Consent Judgment, the following capitalized words or terms shall have the following meanings, which meanings shall apply wherever the words and terms appear in this Consent Judgment:

4. "Action" shall refer to the matter titled Kevin Jespersen, Acting Attorney General of the State of New Jersey, and Steve C. Lee, Director of the New Jersey Division of Consumer Affairs v. Horizon Health Care Services Inc. d/b/a Horizon Blue Cross Blue Shield of New Jersey, Superior Court of New Jersey, Chancery Division, Mercer County, Docket No.:

C12-17, and all pleadings and proceeding related thereto, including the Complaint filed February 15, 2017.

5. "Administrative Safeguards" shall be defined in accordance with 45 C.F.R. §164.304 and are administrative actions, and policies and procedures, to manage the selection, development, implementation and maintenance of security measures to protect Electronic Protected Health Information and to manage the conduct of the Covered Entity's or business associate's workforce in relation to the protection of the information.

6. "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.

7. "Covered Entity" shall be defined in accordance with 45 C.F.R. §106.103 and includes Horizon BCBSNJ.

8. "Division" or "Division of Consumer Affairs" shall refer to the New Jersey Division of Consumer Affairs.

9. "Electronic Protected Health Information" or "ePHI" shall be defined in accordance with 45 C.F.R. §106.103.

10. "Minimum Necessary Standard" shall refer to the requirements of the Privacy Rule that, when using or disclosing Protected Health Information or when requesting Protected Health Information from another Covered Entity, a Covered Entity must make reasonable efforts to limit Protected Health Information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request as defined by 45 C.F.R. § 164.502(b) and § 164.514(d).

11. "Physical Safeguards" shall be defined in accordance with 45 C.F.R. §164.304 and are physical measures, policies and procedures to protect a Covered Entity's electronic

information systems and related buildings and equipment from natural and environmental hazards and from unauthorized intrusion.

12. "Privacy Rule" shall refer to the HIPAA Regulations that establish national standards to safeguard individuals' medical records and other Protected Health Information, including ePHI, that is created, received, used or maintained by a Covered Entity, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E.

13. "Protected Health Information" or "PHI" shall be defined in accordance with 45 C.F.R. §106.103.

14. "Removable Media" shall mean any removable/transportable digital memory medium, such as magnetic tape or disk, optical, or digital memory card, in accordance with the 2nd clause of subparagraph 1 ("electronic media"), as defined in 45 C.F.R. § 160.103

15. "Security Rule" shall refer to the HIPAA Regulations that establish national standards to safeguard individuals' Electronic Protected Health Information that is created, received, used or maintained by a Covered Entity, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and C.

16. "State" shall refer to the State of New Jersey.

17. "Technical Safeguards" shall be defined in accordance with 45 C.F.R. §164.304 and means the technology and the policy and procedures for its use that protect Electronic Protected Health Information and control access to it.

FACTUAL BACKGROUND

18. Horizon BCBSNJ is a domestic corporation with headquarters located at 3 Penn Plaza East, Newark, New Jersey 07105 ("Newark Office"). Horizon BCBSNJ is a major

employer in the State of New Jersey with 5,087 employees across five (5) offices in Newark, Wall, West Trenton, Ewing and Mt. Laurel, New Jersey.

19. Horizon BCBSNJ offers a variety of health insurance plans, including traditional indemnity and managed care plans, such as Health Maintenance Organization, Preferred Provider Organization and Point of Service plans, as well as Medicaid and Medicare coverage. Accordingly, Horizon BCBSNJ is a Health Insurance Issuer, Health Maintenance Organization and/or Health Plan within the meaning of HIPAA. Through such plans, Horizon BCBSNJ provides health insurance coverage to more than 3.7 million New Jersey residents.

20. At all relevant times, Horizon BCBSNJ is and has been a Covered Entity within the meaning of HIPAA.

21. As a Covered Entity, Horizon BCBSNJ is required to comply with the HIPAA federal standards that govern the privacy of individually identifiable health information, including the Privacy Rule and the Security Rule.

22. The Privacy Rule and Security Rule generally prohibit Covered Entities from using or disclosing Protected Health Information and the Privacy Rule requires a Minimum Necessary Standard when Covered Entities use or disclose such Protected Health Information, as well as requiring Covered Entities to employ appropriate Administrative Safeguards, Physical Safeguards and Technical Safeguards to maintain the security and integrity of Protected Health Information.

A. **November 2013 Security Incident:**

23. On Monday, November 4 2013, Horizon BCBSNJ discovered that two unencrypted password-protected laptop computers were stolen from its Newark Office ("November 2013 Incident").

24. The laptops were issued to two (2) employees with the job title "Writer II" and who were employed within Horizon BCBSNJ's marketing division known as the Enterprise Communication Department. A review of the Writer II job description and Horizon BCBSNJ corporate policy reveals that the employees were not required to store ePHI on their laptops in order to perform their job functions. Horizon BCBSNJ policy in effect at the time of the November 2013 Incident limited employee access to ePHI to the minimum necessary to accomplish an employee's job function.

25. Horizon BCBSNJ's review of the November 2013 Incident revealed that the Horizon BCBSNJ employees did not take their password protected, work-issued laptops home over the weekend. Instead, the laptops were cable-locked to the employee workstations, which were located on the 8th floor of Horizon BCBSNJ's Newark Office.

26. At the time of the November 2013 Incident, Horizon BCBSNJ was in the process of renovating its Newark Office and moving various employees. Accordingly, over the weekend of November 1, 2013 through November 3, 2013, approximately thirty-two (32) employees of a vendor moving company had restricted access to Horizon BCBSNJ's Newark Office, including the location of the stolen laptops, as part of the renovations and move. In addition, at least 266 other vendors and/or contractors had restricted access to Horizon BCBSNJ's Newark office, including the location of the stolen laptops, during the same time period. A review of

surveillance footage from the November 2013 Incident revealed non-Horizon BCBSNJ personnel had unsupervised access to the areas from which the laptops were stolen in order to perform the renovation and moving services.

27. Horizon BCBSNJ's investigation of the November 2013 Incident concluded that one or more of the vendor moving company employees may have stolen the laptops. Horizon BCBSNJ shared its findings with the Newark Police Department; however, no arrests have been made.

28. In the course of its review of the November 2013 Incident, Horizon BCBSNJ's investigation revealed that approximately 109 computers assigned to employees were not equipped with Credant volume encryption software ("Credant Software") as required by Horizon BCBSNJ corporate policy. Of these 109 computers, thirty-six (36) contained FileVault Mac encryption software, while ten (10) computers were test machines and did not contain PHI. Following the November 2013 Incident, Horizon BCBSNJ represented that the Credant Software was installed on all company computers within the Enterprise Communications Department.

29. Horizon BCBSNJ's investigation further revealed that the majority of the unencrypted computers were Apple MacBooks procured outside of Horizon BCBSNJ's normal procurement process for the Enterprise Communications Department. Such purchases were not detected by Horizon BCBSNJ's corporate IT department and Horizon BCBSNJ's corporate IT department did not adequately monitor, service or install security software required by corporate policy, including the Credant Software.

30. As a result of the Horizon BCBSNJ IT department's lack of monitoring and servicing of MacBooks within the Horizon BCBSNJ Enterprise Communications Department, an

unauthorized “shadow IT” department developed with respect to the procurement and servicing of certain Mac devices, which was against Horizon BCBSNJ’s existing policies and procedures.

31. Instead of being monitored and serviced by the Horizon BCBSNJ corporate IT department, the MacBooks were monitored by a supervisor of the Enterprise Communications Department. This process was not authorized or approved by Horizon BCBSNJ.

32. As a result of the procurement of the MacBooks outside of Horizon BCBSNJ’s established process, certain MacBooks were not configured with approved encryption, data deletion and other software required by corporate policy.

33. Horizon BCBSNJ subsequently retained the computer forensics investigation firm Navigant Consulting, Inc. (“Navigant”) to conduct an investigation to determine the scope of information contained on the stolen laptops and identify the affected members.

34. Navigant’s investigation revealed that the stolen laptops contained the ePHI of approximately 687,838 New Jersey residents, which included member names, addresses, dates of birth, Horizon BCBSNJ identification numbers and, in some instances, Social Security Numbers and limited clinical information.

35. Horizon BCBSNJ represents that on December 6, 2013 it began notifying affected members by mail and substitute notice in accordance with HIPAA and the New Jersey data breach notification statute, N.J.S.A. 56:8-163. In addition, Horizon BCBSNJ offered affected individuals a free one-year membership in credit monitoring and identity theft protection and restoration services provided by Experian Information Solutions, Inc.

36. On or about December 6, 2013, Horizon BCBSNJ established a dedicated call center to assist impacted members with their questions.

37. On or about December 6, 2013, Horizon BCBSNJ provided notice of the November 2013 Security Incident to the New Jersey State Police, pursuant to N.J.S.A. 56:8-163, the Division, the New Jersey Department of Banking and Insurance and the United States Department of Health and Human Services, Office for Civil Rights.

38. At the time of the November 2013 Incident, Horizon BCBSNJ's corporate policy stated that ePHI on portable devices including laptops and PDAs (including BlackBerry devices) must be encrypted.

B. Additional Security Incidents:

39. Plaintiffs' investigation of the November 2013 Incident revealed that Horizon BCBSNJ had experienced similar laptop thefts and/or other security incidents both prior to and following the November 2013 Incident.

40. On January 7, 2008, Horizon BCBSNJ learned that an IT employee's work-issued unencrypted laptop was stolen at some point over the prior weekend when the employee had brought the laptop home to complete an assignment ("January 2008 Incident").

41. Horizon BCBSNJ's review of the January 2008 Incident revealed that the Horizon BCBSNJ employee had left the laptop in the trunk of his car in violation of corporate policy while attending a church function in Newark. It is believed that the laptop was stolen at that time.

42. The member data compromised in the January 2008 Incident included the ePHI of approximately 300,000 Horizon BCBSNJ members, including names, Social Security Numbers, addresses and dates of birth. Horizon BCBSNJ represents that the laptop involved in the January

2008 Incident was equipped with Absolute Computrace Software, which, after initiated, would delete all member data if the laptop was connected to the internet.

43. Following the January 2008 Incident, Horizon BCBSNJ corporate policy required all company issued laptops to contain encryption software.

44. On or around May 1, 2008, Horizon BCBSNJ issued a statement for the New Jersey Business Journal's Business Safety and Security Spotlight that it had:

[c]ompleted encryption of all its desktop and laptop computers, as well as its mobile devices in an effort to further protect all data within the company. Horizon BCBSNJ employees have also undergone encryption training so that there is a complete understanding of the new security measures that have been adopted.

45. On or about March 28, 2012, Horizon BCBSNJ discovered that a subcontractor that provided claim processing services to Horizon BCBSNJ included the ePHI of approximately thirteen (13) Horizon BCBSNJ members in a test claim file that was posted to a publicly available website. Access to ePHI was not required for the subcontractor to perform his job duties.

46. On June 12, 2012, a Horizon BCBSNJ vendor left an unencrypted vendor-issued laptop in a New York taxi cab. The vendor's employee had previously downloaded Horizon BCBSNJ member ePHI onto the lost laptop, against Horizon BCBSNJ policy. Horizon BCBSNJ's review of the incident revealed that the laptop contained the ePHI of approximately eleven (11) New Jersey residents and that the subcontractor did not need access to ePHI to perform his job duties.

C. Violations of Law:

47. The Division's investigation identified that Horizon BCBSNJ, as described above, engaged in multiple violations of the CFA, HIPAA, the Privacy Rule and Security Rule.

48. By its actions as described above, Horizon BCBSNJ failed to comply with the following standards, Administrative Safeguards, Physical Safeguards, Technical Safeguards and implementation specifications as required by HIPAA, the Privacy Rule and the Security Rule:

- a. Horizon BCBSNJ failed to review and modify security measures as needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. §164.306(e).
- b. Horizon BCBSNJ failed to conduct an accurate and thorough risk assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI it held, in violation of 45 C.F.R. §164.308(a)(1)(ii)(A).
- c. Horizon BCBSNJ failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Rule, in violation of 45 C.F.R. §164.308(a)(1)(ii)(B).
- d. Horizon BCBSNJ failed to apply appropriate sanctions against workforce members who failed to comply with its security policies and procedures, in violation of 45 C.F.R. §164.308(a)(1)(ii)(C).
- e. Horizon BCBSNJ failed 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)(D).
- f. Horizon BCBSNJ failed to implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed, in violation of 45 C.F.R. §164.308(a)(3)(ii)(A).

- g. Horizon BCBSNJ failed to implement procedures to determine that the access of a workforce member to ePHI is appropriate, in violation of 45 C.F.R. §164.308(a)(3)(ii)(B).
- h. Horizon BCBSNJ failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review and modify a user's right of access to a workstation, transaction, program or process that includes ePHI, in violation of 45 C.F.R. §164.308(a)(4)(ii)(C).
- i. Horizon BCBSNJ failed to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that were known to it; and document security incidents and their outcomes, in violation of 45 C.F.R. §164.308(a)(6)(ii).
- j. Horizon BCBSNJ failed to implement a periodic technical and nontechnical evaluation in response to environmental or operational changes affecting the security of ePHI that establishes the extent to which its security policies and procedures meet the requirements of the Security Rule, in violation of 45 C.F.R. §164.308(a)(8).
- k. Horizon BCBSNJ failed to implement policies and procedures to safeguard its facility and the equipment therein from unauthorized physical access, tampering and theft, in violation of 45 C.F.R. §164.310(a)(2)(ii).
- l. Horizon BCBSNJ failed to implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, in violation of 45 C.F.R. §164.301(a)(2)(iii).
- m. Horizon BCBSNJ failed to implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI, in violation of 45 C.F.R. §164.310(b).
- n. Horizon BCBSNJ failed to implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users, in violation of 45 C.F.R. §164.310(c).
- o. Horizon BCBSNJ failed to maintain a record of the movements of hardware and electronic media containing ePHI and any person responsible therefore, in violation of 45 C.F.R. §164.310(d)(2)(iii).

- p. Horizon BCBSNJ failed to implement a mechanism to encrypt and decrypt ePHI, in violation of 45 C.F.R. §164.312(a)(2)(iv).
- q. Horizon BCBSNJ failed to implement hardware, software and/or procedural mechanisms that record and examine activity that contain or use ePHI, in violation of 45 C.F.R. §164.312(b).
- r. Horizon BCBSNJ failed to implement policies and procedures to protect ePHI from improper alteration or destruction, in violation of 45 C.F.R. §164.312(c)(1).
- s. Horizon BCBSNJ failed to implement a mechanism to encrypt ePHI whenever deemed appropriate, in violation of 45 C.F.R. §164.312(e)(2)(ii).
- t. Horizon BCBSNJ violated the Privacy Rule, 45 C.F.R. §164.502 et seq.
- u. Horizon BCBSNJ failed to adhere to the Minimum Necessary Standard when using or disclosing PHI, in violation of 45 C.F.R. §164.502(b)(1).
- v. Horizon BCBSNJ failed to adequately train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain the security of PHI, in violation of 45 C.F.R. §164.530(b)(1).
- w. Horizon BCBSNJ failed to reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of the Privacy Rule, in violation of 45 C.F.R. §164.530(c)(2)(i).
- x. Horizon BCBSNJ failed to apply appropriate sanctions against members of its workforce who failed to comply with its privacy policies and procedures or the requirement of the Privacy Rule, in violation of 45 C.F.R. §164.530(e)(1).

49. Each of the above-referenced practices by Horizon BCBSNJ constitutes additional and separate unconscionable commercial practices in violation of the CFA, N.J.S.A. 56:8-2.

50. In addition, Horizon BCBSNJ has engaged in the following false promises and misrepresentations in violation of the CFA, N.J.S.A. 56:8-2:

- a. Representing that it maintained appropriate Administrative Safeguards, Technical Safeguards and Physical Safeguards to protect its members PHI, when such was not the case.
- b. Representing that all Horizon BCBSNJ laptop computers containing PHI would be fully encrypted, when such was not the case.
- c. Representing that Horizon BCBSNJ had completed encryption of all laptop computers, when such was not the case.
- d. Representing that all Horizon BCBSNJ employees had been appropriately trained on encryption, when such was not the case.
- e. Following the January 2008 Incident, Horizon BCBSNJ represented it would take additional measures to prevent further laptop thefts. However, such measures were either not taken or ineffective.

BUSINESS PRACTICES AND INJUNCTIVE RELIEF

51. Horizon BCBSNJ shall not engage in any unfair or deceptive acts or practices in the conduct of its business in the State and shall comply with all applicable State and/or Federal laws, rules and regulations as now constituted or as may hereafter be amended including, but not limited to, the CFA and HIPAA.

52. Horizon BCBSNJ shall comply with all Administrative Safeguards, Physical Safeguards, Technical Safeguards and implementation specifications required by HIPAA, the Privacy Rule and the Security Rule, including those safeguards and specifications enumerated in Paragraph 48 of this Consent Judgment.

53. Horizon BCBSNJ shall be responsible for the performance of the following Corrective Action Plan ("CAP"). The period for compliance with the obligations assumed under

the CAP shall begin on the Effective Date of this Consent Judgment and end two (2) years from the Effective Date.

54. As part of the CAP, within ninety (90) days of the Effective Date, and thereafter annually for a period of one (1) additional year, Horizon BCBSNJ shall engage an independent third-party professional who uses procedures and standards generally accepted in the profession to conduct a current, comprehensive and thorough risk analysis of security risks and vulnerabilities to member ePHI present in Horizon BCBSNJ facilities, Removable Media, policies and practices for handling, containing, storing, transmitting and/or receiving ePHI, including a review of the actions that are the subject of this Consent Judgment. The independent third-party professional conducting the risk analysis shall prepare a formal report including its findings and recommendations to be submitted to Horizon BCBSNJ and the Division ("Security Report"). The initial Security Report shall be submitted to Horizon BCBSNJ and the Division no later than one hundred eighty (180) days of the Effective Date and each subsequent Security Report shall be submitted on the anniversary thereof.

55. Within ninety (90) days of its receipt of each Security Report, Horizon BCBSNJ shall review and, to the extent necessary, revise its current policies and procedures based on the findings of the Security Report. Horizon BCBSNJ shall forward to the Division any action it takes, or if no action is taken, a detailed description why no action is necessary, in response to each Security Report within one hundred twenty (120) days of Horizon BCBSNJ's receipt of each Security Report ("Horizon BCBSNJ Action Report").

56. As part of the CAP and in addition to its current policies and procedures, as well as those developed in response to the recommendations in each Security Report, Horizon

BCBSNJ shall strengthen its managerial oversight to comply with the Minimum Necessary Standard. Specifically, Horizon BCBSNJ's privacy officer or other designated official shall catalogue, review and monitor all Horizon BCBSNJ Removable Media, whether or not such media contains PHI.

57. The privacy officer or designated official shall, in accordance with HIPAA, make reasonable efforts to ensure: (a) the identification of those workforce members that need access to PHI to perform their job functions and limit access to PHI to those workforce members; (b) all Horizon BCBSNJ Removable Media containing ePHI is properly supervised, catalogued and documented; (c) all Horizon BCBSNJ Removable Media is equipped with appropriate encryption and other software, as necessary; (d) report any known violations of Horizon BCBSNJ policies and procedures relating to the HIPAA Minimum Necessary Standard, as set forth in 45 C.F.R. § 164.502(b) and § 164.514(d), to the appropriate Horizon BCBSNJ official and remediate any known violations as soon as practicable; (e) all member records that are no longer necessary to retain are destroyed in accordance with HIPAA and/or the CFA; and (f) for a period of two (2) years, report security incidents involving the loss or compromise of New Jersey residents' PHI to the Attorney General that might not otherwise trigger the reporting requirements of N.J.S.A. 56:8-161 to -166, but only where such loss or compromise of PHI also triggers notification requirements under HIPAA.

58. The findings of the privacy officer or other designated official concerning Horizon BCBSNJ's compliance with the Minimum Necessary Standard and those specific issues addressed in Paragraph 57 shall be included as a separate section in each Horizon BCBSNJ Action Report submitted to the Division.

SETTLEMENT AMOUNT

59. The Parties have agreed to a settlement of this Action in the amount of One Million One Hundred Thousand and 00/100 Dollars (\$1,100,000.00) ("Settlement Amount").

60. The Settlement Amount comprises Nine Hundred Twenty Six Thousand Eight Hundred Three and 22/100 Dollars (\$926,803.22) in civil penalties, pursuant to N.J.S.A. 56:8-13 and HIPAA, Seventy Thousand Sixty Eight and 50/100 Dollars (\$70,068.50) in reimbursement of Plaintiffs' attorneys fees and Twenty Three Thousand One Hundred Twenty Eight and 28/100 Dollars (\$23,128.28) investigative costs, pursuant to N.J.S.A. 56:8-11, 56:8-19 and HIPAA and Eighty Thousand and 00/100 Dollars (\$80,000.00) to be used at the sole discretion of the Attorney General for the promotion of consumer privacy programs and/or the enforcement of consumer privacy initiatives, including but not limited to, the purchase of investigative tools, the retention of technologists, consultants and experts, staff training and education, and the retention of additional staff and resources dedicated to privacy enforcement.

61. The Settlement Amount only includes calculations, payments or penalties associated with the November 2013 Security Incident and does not include any such calculations, payments or penalties for other security incidents that occurred prior to 2009.

62. Horizon BCBSNJ shall pay Nine Hundred Fifty Thousand and 00/100 Dollars (\$950,000.00) of the Settlement Amount ("Settlement Payment"), no later than seven (7) business days after Horizon BCBSNJ receives notification that this Consent Judgment has been entered by the Court.

63. The Settlement Payment shall be made by credit card, wire transfer, bank check, money order, certified check, or cashier's check payable to "New Jersey Division of Consumer Affairs" and shall be forwarded to:

Van Mallett
Case Management Tracking
Division of Consumer Affairs
124 Halsey Street – 7th Floor
P.O. Box 45024
Newark, New Jersey 07101

64. Upon making the Settlement Payment, Horizon BCBSNJ shall immediately be fully divested of any interest in, or ownership of, the monies paid and all interest in the monies, and any subsequent interest or income derived therefrom, shall inure entirely to the benefit of the Plaintiffs pursuant to the terms herein.

65. The balance of the Settlement Amount, totaling One Hundred Fifty Thousand and 00/100 Dollars (\$150,000.00) and consisting of civil penalties and attorneys' fees, shall be suspended and automatically vacated ("Suspended Penalty") at the expiration of two (2) years from the Effective Date, provided:

- a. Horizon BCBSNJ complies in all material respects with the CAP, described at Paragraphs 52 – 58 of this Consent Judgment; and
- b. Horizon BCBSNJ complies in all material respects with the terms and conditions set forth in this Consent Judgment. However, for the purposes of this Consent Judgment, any HIPAA violations by Horizon BCBSNJ, including but not limited to, any breach of protected health information, that are not due to "willful neglect" as that term is defined in HIPAA at 45 C.F.R. §160.401, are not material violations of the terms and conditions set forth in this Consent Judgment, nor shall any such HIPAA violations be deemed to violate the CFA.

66. In the event Horizon BCBSNJ fails to comply with Paragraph 65 of this Consent Judgment, Plaintiffs shall provide Horizon BCBSNJ with written notice of default or noncompliance, seeking payment of any unpaid portion of the Settlement Payment, as well as

the Suspended Penalty ("Notice of Noncompliance"). In any such Notice of Noncompliance, Plaintiffs shall provide Horizon BCBSNJ with the specific details of the alleged default or noncompliance, as well as any supporting documents, and shall afford Horizon BCBSNJ a sixty (60) day period from receipt of the Notice of Noncompliance within which to cure the default or noncompliance. Plaintiffs may move on short notice or by Order to Show Cause to have a judgment entered for any unpaid portion of the Settlement Payment as well as the Suspended Penalty.

67. For the purposes of this Consent Judgment, the security incident which occurred on or around November 1, 2016 and was announced by Horizon BCBSNJ on November 14, 2016 ("November 2016 Incident") shall not constitute a failure to comply with Paragraph 65.

DISMISSAL OF ACTION

68. The entry of this Consent Judgment constitutes a dismissal with prejudice of the Action.

GENERAL PROVISIONS

69. This Consent Judgment 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 Judgment.

70. This Consent Judgment shall be governed by, and construed and enforced in accordance with, the laws of this State.

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

72. This Consent Judgment contains the entire agreement among the Parties. Except as otherwise provided herein, this Consent Judgment shall be modified only by a written instrument signed by or on behalf of the Plaintiffs and Horizon BCBSNJ.

73. Except as otherwise explicitly provided for in this Consent Judgment, 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.

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

75. This Consent Judgment 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 Judgment avoid compliance with this Consent Judgment.

76. This Consent Judgment is agreed to by the Parties and entered into for settlement purposes only. Neither the fact of, nor any provision contained in this Consent Judgment nor any action taken hereunder 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 Horizon BCBSNJ; and (b) an admission by Horizon BCBSNJ that any of its acts or practices described herein or prohibited by this Consent Judgment are unfair or deceptive or violate HIPAA or any consumer protection law of the State, including the CFA. This Consent Judgment is not intended, and shall not be deemed, to constitute evidence or precedent of any kind except in: (a) any action or proceeding by one of the Parties to enforce, rescind or otherwise implement or affirm any or all terms of this Consent Judgment; or (b) any action or proceeding involved a Released Claim (as defined in Paragraph 80, below) to support a

defense of res judicata, collateral estoppel, release or other theory of claim preclusion, issue preclusion or similar defense.

77. Nothing contained in this Consent Judgment shall be construed to limit or otherwise affect the rights of any persons who are not Parties to this Consent Judgment with respect to any of the matters contained herein.

78. The Parties represent and warrant that their signatories to this Consent Judgment have authority to act for and bind the respective Parties.

79. Unless otherwise prohibited by law, any signatures by the Parties required for entry of this Consent Judgment may be executed in counterparts, each of which shall be deemed an original, but all of which shall together be one and the same Consent Judgment.

RELEASE

80. In consideration of the payments, undertakings, mutual promises and obligations provided for in this Consent Judgment and conditioned on Horizon BCBSNJ making the Settlement Payment, Plaintiffs hereby agree to release Horizon BCBSNJ from any and all civil claims or consumer related administrative claims, to the extent permitted by State law, which Plaintiffs could have brought against Horizon BCBSNJ for violations of the CFA and/or HIPAA arising out of the Complaint, regardless of whether such violations were included in the calculation of the Settlement Amount, as well as all of the matters specifically addressed in this Consent Judgment ("Released Claims").

81. Notwithstanding any term of this Consent Judgment, the following do not comprise Released Claims: (a) private rights of action; (b) actions to enforce this Consent

Judgment; (c) any claims against Horizon BCBSNJ by any other agency or subdivision of the State; and (d) the November 2016 Incident.

PENALTIES FOR FAILURE TO COMPLY

82. The Attorney General (or designated representative) shall have the authority to enforce the provisions of this Consent Judgment or to seek violations hereof or both.

COMPLIANCE WITH ALL LAWS

83. Except as provided in this Consent Judgment, no provision herein shall be construed as:

- (a) Relieving Horizon BCBSNJ of its obligations to comply with all State and Federal laws, regulations or rules, as now constituted or as may hereafter be amended, or as granting permission to engage in any acts or practices prohibited by any such laws, regulations or rules; or
- (b) Limiting or expanding any right the Plaintiffs may otherwise have to obtain information, documents or testimony from Horizon BCBSNJ pursuant to any State or Federal law, regulations or rule, as now constituted or as may hereafter be amended, or limiting or expanding any right Horizon BCBSNJ may otherwise have pursuant to any State or Federal law, regulation or rule, to oppose any process employed by the Plaintiffs to obtain such information, documents or testimony.

NOTICES UNDER THIS CONSENT JUDGMENT

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

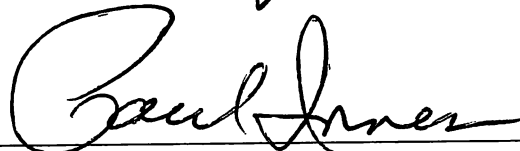
For the Plaintiffs:

Elliott M. Siebers, Deputy Attorney General
Russell M. Smith, Jr., Deputy Attorney General
State of New Jersey
Office of the Attorney General
Department of Law and Public Safety
Division of Law
124 Halsey Street – 5th Floor
P.O. Box 45029
Newark, New Jersey 07101

For Horizon BCBSNJ:

Theodore J. Kobus III, Esq.
Eric A. Packel, Esq.
Baker & Hostetler LLP
45 Rockefeller Plaza
New York, New York 10111

IT IS ON THE 15th DAY OF February 2017 SO ORDERED,
ADJUDGED AND DECREED.

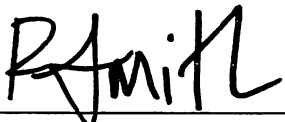
A handwritten signature in black ink, appearing to read "Paul Innes", written over a horizontal line.

HON. PAUL INNES, P.J. Ch.

**JOINTLY APPROVED AND
SUBMITTED FOR ENTRY:**

FOR THE PLAINTIFFS:

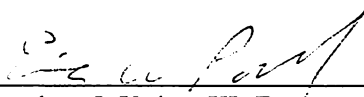
KEVIN JESPERSEN
ACTING ATTORNEY GENERAL OF NEW JERSEY

By: 
Elliott M. Siebers
Russell M. Smith, Jr.
Deputy Attorneys General
Brian McDonough
John M. Falzone
Assistant Attorneys General
Division of Law
124 Halsey Street, 5th Floor
Newark, New Jersey 07101

Dated: 2/10, 2017

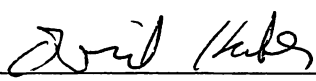
FOR HORIZON BCBSNJ:

BAKER & HOSTETLER, LLP

By: 
Theodore J. Kobus III, Esq.
Eric A. Packel, Esq.
45 Rockefeller Plaza
New York, New York 10111

Dated: 2/6, 2017

HORIZON HEALTHCARE SERVICES, INC.,
d/b/a HORIZON BLUE CROSS BLUE SHIELD OF NEW JERSEY

By:  Dated: February 2, 2017

Name: David Huber

Title or Position: Senior Vice President and Chief Financial Officer

Address: 3 Penn Plaza East Newark, NJ 07105