

GURBIR S. GREWAL
ATTORNEY GENERAL OF NEW JERSEY
Division of Law
124 Halsey Street, 5th Floor
P.O. Box 45029
Newark, New Jersey 07101
Attorney for Division of Consumer Affairs

FILED

NOV 28 2018

Division of Consumer Affairs

By: Lara J. Fogel
Deputy Attorney General
(973) 648-2865

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

In the Matter of

Administrative Action

GROUP HEALTH INCORPORATED
AND EMBLEMHEALTH, INC.,

CONSENT ORDER

Respondents.

WHEREAS this matter was opened by the New Jersey Division of Consumer Affairs, Office of Consumer Protection (“Division”), as an investigation to ascertain whether violations of the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 et seq. (“CFA”), the New Jersey Identity Theft Prevention Act, N.J.S.A. 56:8-161 et seq. (“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 et seq. (collectively, “HIPAA”), have been or are being committed by Group Health Incorporated (“GHI”) and EmblemHealth, Inc., (collectively, “EmblemHealth” or “Respondents”) (hereinafter referred to as the “Investigation”);

WHEREAS the Division has alleged that EmblemHealth engaged in conduct in violation of the ITPA, CFA and HIPAA in connection with EmblemHealth's improper display of Medicare Health Insurance Claim Numbers, which mirror individual social security numbers, belonging to 81,122 of its policyholders, 6,443 of whom were New Jersey residents; and

WHEREAS the Division and Respondents (collectively, "Parties") have reached an amicable agreement resolving the issues in controversy and concluding the Investigation without the need for further action, and Respondents have voluntarily cooperated with the Investigation and consented to the entry of the within order ("Consent Order") without having admitted 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 ("Effective Date").

2. DEFINITIONS

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

2.1 "Administrative Safeguards" shall be defined in accordance with 45 C.F.R. § 164.304 and Includes administrative actions and Policies to manage the selection, development, implementation and maintenance of security measures to protect e-PHI and to manage the conduct of the Covered Entity's or Business Associate's workforce in relation to the protection of the information.

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 of Security” shall be defined in accordance with N.J.S.A. 56:8-161.

2.4 “Business” shall be defined in accordance with N.J.S.A. 56:8-161.

2.5 “Business Associate” shall be defined in accordance with 45 C.F.R. § 106.103.

2.6 “Covered Entity” shall be defined in accordance with 45 C.F.R. § 106.103 and Includes Respondents.

2.7 “Customer” shall be defined in accordance with N.J.S.A. 56:8-161.

2.8 “Electronic Protected Health Information” or “e-PHI” shall be defined in accordance with 45 C.F.R. § 160.103, and Includes any information transmitted or maintained in electronic media that is created or received by a Covered Entity relating to the physical or mental health of an Individual and for which there is a reasonable basis to believe the information can be used to identify the Individual.

2.9 “HICN” is a Medicare beneficiary’s Health Insurance Claim Number.

2.10 “Include” and “Including” shall be construed as broadly as possible and shall mean “without limitation.”

2.11 “Individual” shall be defined in accordance with 45 C.F.R. § 160.103 and N.J.S.A. 56:8-161.

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

2.13 “New Jersey Customer” shall refer to a Customer who is a resident of New Jersey.

2.14 “Personal Information” shall be defined in accordance with N.J.S.A. 56:8-161.

2.15 “Person” shall be defined in accordance with N.J.S.A. 56:8-1(d).

2.16 “Policy” or “Policies” shall include any procedures, practices and/or established courses of action, whether written or oral.

2.17 “Privacy Rule” shall refer to the HIPAA regulations that establish national safeguards to safeguard Individuals’ medical records and other PHI 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.

2.18 “Protected Health Information” or “PHI” shall be defined in accordance with 45 C.F.R. § 106.103, and Includes any information created or received by a Covered Entity relating to the physical or mental health of an Individual and for which there is a reasonable basis to believe the information can be used to identify the Individual.

2.19 “Security Rule” shall refer to the HIPAA regulations that establish national standards to safeguard Individuals’ e-PHI 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.

2.20 “SSN[s]” shall refer to social security number[s].

3. STIPULATED FINDINGS OF FACTS

3.1 GHI is a New York not-for-profit corporation that provides health care coverage and administrative services to employers and individuals located in the State of New York, with Customers who reside in New Jersey. It is a wholly-owned subsidiary of EmblemHealth, Inc. Both companies maintain a principal business address at 55 Water Street, New York, New York 10041.

3.2 On or about October 3, 2016, EmblemHealth's vendor mailed a paper copy of EmblemHealth's Medicare Part D Prescription Drug Plan's Evidence of Coverage (the "2016 EOC Mailing") to 81,122 of its Customers, 6,443 of which were New Jersey Customers.

3.3 The mailing label affixed to the 2016 EOC Mailing improperly Included each Customer's HICN, which incorporates the 9-digits of the Customer's SSN, as well as an alphabetic or alphanumeric beneficiary identification code ("BIC"). The number shown was identified as the "Package ID#" on the mailing label and did not include any separation between the digits.

3.4 On or about October 13, 2016, EmblemHealth learned that the Customers' HICNs had been exposed on the mailing labels of the EOCs and recognized it as a privacy incident.

3.5 The Division's Investigation found that during the normal course of business, a trained EmblemHealth employee under appropriate supervision would retrieve an internally generated data file that Included HICNs as an internal EmblemHealth identification of each Customer, and then engage in a critical two-step process: (i) remove the HICNs field, and (ii) add a Mailing ID field instead. The employee would then send this modified file without the HICN to EmblemHealth's print vendor and Business Associate, The Sourcing Group ("TSG"), which would use the Mailing IDs to auto-generate machine-readable barcodes for EmblemHealth's mailing vendor, United Parcel Service Mailing Innovations ("UPSMI"). UPSMI would use the barcode to generate mailing labels to be affixed to the outside of the envelopes. EmblemHealth would begin this process in May of each year to complete the EOC mailing by a September 30th deadline.

3.6 The EmblemHealth employee who typically prepared the EOC mailings resigned sometime prior to the 2016 EOC Mailing. Accordingly, the 2016 EOC Mailing was assigned to a team manager of EmblemHealth's Medicare Products Department. Creation and transmission of the data file was not part of that team manager's normal responsibilities. The team manager received minimal job-specific training relating to this task, and was not subject to any supervision or oversight concerning the creation or transmission of the data file to TSG.

3.7 In documents that EmblemHealth provided to the Division on or about August 31, 2017, in connection with the Investigation, EmblemHealth represented that there was an internal "written process documentation" setting forth a protocol for how to manage the EOC mailing data requests.

3.8 In documents that EmblemHealth provided to the Division on or about April 27, 2018, in connection with the Investigation, EmblemHealth admitted that this "written process documentation" did not set forth the two-step process of adding a Mailing ID field and removing the HICN field.

3.9 On or about October 3, 2016, the team manager neglected to: (a) remove the patient HICNs, and (b) add the Mailing ID field to the electronic file sent to TSG.

3.10 Subsequently, TSG notified the team manager that the electronic file was improperly formatted because TSG did not see the Mailing ID field. The team manager failed to address TSG's concern, and instead instructed TSG to use another field and proceed with the process of creating barcodes for UPSMI. TSG selected the HICN field to use to create the barcodes for UPSMI because it was one of the first fields to appear in the file.

3.11 Prior to sending the hard-copy packages to UPSMI for mailing, and consistent with EmblemHealth's policy and procedure at the time, TSG sent the Medicare Products Department manager samples of the package fly sheets to review. The fly sheet contained the member's name, address and barcode, but did not include the mailing label, which was generated and printed by UPSMI.

3.12 On October 3, 2016, using the barcode created by TSG, UPSMI printed mailing labels that Included Customers' HICNs, affixed the labels to the front of envelopes, and mailed the envelopes to, among others, 6,443 EmblemHealth Customers who reside in New Jersey. The HICNs (identified as the "Package ID#") Included the 9-digits of the Customers' SSN, which were visible as a series of numbers without hyphens on the envelope mailing label.

3.13 EmblemHealth promptly notified affected Customers in November 2016 and offered them two years of free credit monitoring and identity protection services. EmblemHealth also contracted with its identity protection vendor to staff a dedicated helpline to assist with any Customer questions or concerns.

3.14 In addition, EmblemHealth implemented several corrective measures Including the following:

- a) the employee who made the inadvertent disclosure was re-educated and disciplined and, in November 2016, the Chief Compliance Officer conducted an in-person training for the Medicare Products Department team to reinforce the Policies relevant to the team, Including those related to the mailing at issue here;
- b) EmblemHealth updated and enhanced existing Policies and internal processes to Include more detailed language and strengthen internal controls regarding the safeguarding of e-PHI; and
- c) EmblemHealth increased the frequency with which it issues "compliance reminders" to all employees via email or intranet.

4. ALLEGED VIOLATIONS OF LAW

4.1 The Division's Investigation identified that EmblemHealth, as described above, violated the ITPA (see N.J.S.A. 56:8-164; N.J.A.C. 13:45F-4.1) when, in connection with the 2016 EOC Mailing, it displayed its Customers' HICNs as a Package ID# on the outside mailing label of the packages.

4.2 The Division's finding that EmblemHealth violated the ITPA led the Division to conclude that violations of the CFA also occurred (see N.J.S.A. 56:8-166; N.J.A.C. 13:45F-5.2).

4.3 The Division's Investigation also identified that EmblemHealth, as described above, engaged in multiple violations of HIPAA.

4.4 At all relevant times, EmblemHealth is, and has been, a Covered Entity within the meaning of HIPAA.

4.5 As a Covered Entity, EmblemHealth is required to comply with the standards and procedural specifications, as required by HIPAA, the Privacy Rule and the Security Rule.

4.6 The Security Rule establishes national standards required to safeguard Individuals' e-PHI that is created, received, used or maintained by a Covered Entity.

4.7 The Privacy Rule establishes national standards required to safeguard Individuals' PHI that is created, received, used or maintained by a Covered Entity.

4.8 These rules prohibit Covered Entities from disclosing PHI, and require the implementation of a minimum necessary standard, including the use of appropriate administrative, physical and technical safeguards to maintain the security and integrity of PHI.

4.9 By its conduct, as described above, EmblemHealth failed to comply with the following standards and procedural specifications, as required by HIPAA, the Privacy Rule and the Security Rule:

- a. EmblemHealth's Medicare Products Department failed to maintain the confidentiality of the subject ePHI, and failed to protect adequately against the reasonably anticipated use or disclosure of the subject ePHI not permitted under the Privacy Rule, and failed to ensure compliance with the Security Rule. See 45 C.F.R. § 164.306(a) and (c);
- b. EmblemHealth failed to implement adequate procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where ePHI might be accessed, in violation of 45 C.F.R. § 164.308(a)(3)(ii)(A), or alternatively failed to document why it would not be reasonable and appropriate to implement the procedures and implement an equivalent alternative measure if reasonable and appropriate, as required by 45 C.F.R. § 164.306(d)(3)(ii)(B);
- c. EmblemHealth failed to conduct an accurate and thorough risk assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI it holds, in violation of 45 C.F.R. § 308(a)(1)(ii)(A);
- d. EmblemHealth failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 45 C.F.R. § 164.306(c), in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B);
- e. EmblemHealth failed to respond to a suspected or known security incident that was duly reported to it by their Business Associate pursuant to 45 C.F.R. §§ 164.314(a)(2)(i)(C) and 164.410(a), in violation of 45 C.F.R. § 164.308(a)(6)(ii);
- f. EmblemHealth's Medicare Products Department improperly disclosed PHI in violation of 45 C.F.R. § 164.502(a);
- g. EmblemHealth's Medicare Products Department failed to adhere to the minimum necessary standard when it disclosed PHI to its Business Associate, in violation of 45 C.F.R. § 164.502(b);
- h. EmblemHealth failed to have available an adequately trained member of its Medicare Products Department for the 2016 EOC Mailing project team when the assigned employee resigned, in violation of 45 C.F.R. § 164.530(b)(1); and
- i. EmblemHealth, in connection with the 2016 EOC Mailing, failed to have in place appropriate Administrative Safeguards to protect the privacy of

PHI, failed to reasonably safeguard PHI from any unintentional use or disclosure that is in violation of the standards, implementation specifications, or other requirement of the Privacy Rule, and failed to reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure, in violation of 45 C.F.R. § 164.530(c).

4.10 EmblemHealth admits the factual findings in Section 3 above, and, in the interests of resolving this Investigation without the necessity of prolonged proceedings, neither admits nor denies the Division's Alleged Violations of Law in Section 4.

5. REQUIRED AND PROHIBITED BUSINESS PRACTICES

5.1 EmblemHealth shall comply with all applicable State and/or Federal laws, rules and regulations, as now constituted or as may hereafter be amended, Including the ITPA, CFA, HIPAA, the Security Rule and/or the Privacy Rule.

5.2 EmblemHealth shall not engage in conduct in violation of the ITPA, CFA, HIPAA, the Security Rule and/or the Privacy Rule.

5.3 EmblemHealth shall notify New Jersey Customers of any Breach of Security in the most expedient time possible and without unreasonable delay, as required by the ITPA, specifically N.J.S.A. 56:8-163(a).

5.4 As of the Effective Date, and for three years thereafter, for any Breach of Security of the Personal Information of New Jersey Customers, EmblemHealth shall provide notice to the Division, as provided in Section 12.1, in addition to any other requirements of the ITPA.

6. COMPLIANCE REQUIREMENTS

6.1 To the extent it has not already done so, EmblemHealth will satisfy in full all aspects of the Compliance Provisions detailed in Sections 6.2 through 6.7 within one hundred and twenty (120) days of the Effective Date.

6.2 EmblemHealth will no longer use HICNs that Include SSNs and/or Medicare Beneficiary Identifiers (“MBIs”) to identify Customers in mailing files. Instead, EmblemHealth will convert to a system that utilizes unique identifiers to identify its Customers.

6.3 EmblemHealth will revise its Policies, Including its Policy related to standards of conduct, to prohibit the use of SSNs, HICNs and MBIs in mailing files, and to further prohibit any public disclosure of SSNs, HICNs or MBIs. EmblemHealth will explicitly Include this prohibition when defining Minimum Necessary requirements in its Policies. (See 45 C.F.R. 164.502 (b).)

6.4 EmblemHealth will revise its Policies, Including checklists, to require transitioning an outgoing employee’s responsibilities to another qualified employee or third party. This transition process will Include necessary training.

6.5 EmblemHealth will engage a training vendor and will implement new privacy and security training modules to all employees, among other things, which training shall:

- a. Define Minimum Necessary requirements with respect to prohibition of disclosure of SSNs, HICNs and MBIs in mailing files, and any public disclosure of SSNs, HICNs or MBIs;
- b. Contain content explicitly devoted to management during employee transition, Including specific language related to the employment termination Policy and transition of work when an employee separates from the company; and
- c. Contain content stating that encryption is mandatory.

6.6 At a minimum, EmblemHealth shall conduct the training referenced in Section 6.5 for each employee upon hiring, and on an annual basis thereafter.

6.7 All employees of EmblemHealth, Including supervisory employees, will receive the training referenced in Sections 6.5 through 6.6.

7. SETTLEMENT PAYMENT

7.1 The Parties have agreed to a settlement of the Investigation in the amount of One Hundred Thousand Dollars (\$100,000.00) (“Settlement Payment”), which consists of a civil penalty pursuant to N.J.S.A. 56:8-13.

7.2 EmblemHealth shall make the Settlement Payment contemporaneously with the signing of this Consent Order.

7.3 EmblemHealth shall make the Settlement Payment by certified check, cashier’s check, money order, credit card or wire transfer 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

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

8. GENERAL PROVISIONS

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

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

8.3 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.

8.4 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.

8.5 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.

8.6 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.

8.7 This Consent Order shall be binding upon Respondents, as well as their owners, officers, directors, representatives, managers, agents, employees, successors and assigns, and any Persons through which they may now or hereafter act, as well as any Persons who have authority to control or who, in fact, control and direct their Business.

8.8 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.

8.9 This Consent Order is agreed to by the Parties and entered into 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 Division or any other governmental unit of the State of any act or practice of Respondents; or (b) an admission by Respondents that they violated the ITPA, CFA, HIPAA, the Privacy Rule and/or the Security Rule.

8.10 This Consent Order is not intended, and shall not be deemed, to constitute evidence or precedent of any kind except in: (a) an action or proceeding by one of the Parties to enforce, rescind or otherwise implement any or all of the terms herein; or (b) an action or proceeding involving a Released Claim (as defined in Section 9) to support a defense of res judicata, collateral estoppel, release or other theory of claim preclusion, issue preclusion or similar defense.

8.11 The Parties represent and warrant an authorized representative of each has signed this Consent Order with full knowledge, understanding and acceptance of its terms and that the representative has done so with authority to legally bind the respective Party.

8.12 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.

8.13 This Consent Order is a public document subject to the New Jersey Open Public Records Act, N.J.S.A. 47:1A-1 et seq.

9. RELEASE

9.1 In consideration of the undertakings, mutual promises and obligations provided for in this Consent Order and conditioned on Respondents making the Settlement Payment in the

manner specified above, the Division hereby agrees to release Respondents from any and all civil claims or Consumer-related administrative claims, to the extent permitted by State law, which the Division could have brought prior to the Effective Date against Respondents for violations of the CFA, the ITPA, HIPAA, the Privacy Rule and/or the Security Rule arising out of the Investigation, the 2016 EOC Mailing, as well as the matters specifically addressed in this Consent Order (“Released Claims”).

9.2 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 Respondents by any other agency or subdivision of the State.

10. PENALTIES FOR FAILURE TO COMPLY

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

11. COMPLIANCE WITH ALL LAWS

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

- a. Relieving Respondents of their 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 Division may otherwise have to obtain information, documents or testimony from Respondents 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 Respondents 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.

12. NOTICES

12.1 Except as otherwise provided herein, any notices or other documents required to be sent to the Division or Respondents 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. The notices and/or documents shall be sent to the following addresses:

For the Division:

Lara J. Fogel
Deputy Attorney General
Office of the Attorney General
Department of Law and Public Safety
124 Halsey Street, 5th Floor
P.O. Box 45028
Newark, New Jersey 07101

For Respondents:

Debra M. Lightner
Senior Vice President and Chief Compliance Officer
EmblemHealth
55 Water Street
New York, New York 10041

IT IS ON THE 28 DAY OF November, 2018 SO ORDERED.

GURBIR S. GREWAL
ATTORNEY GENERAL OF NEW JERSEY

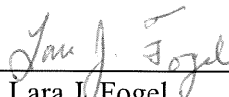
By: 

PAUL R. RODRÍGUEZ, 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.**

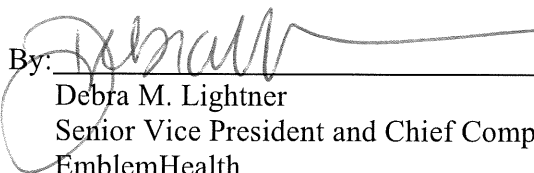
FOR THE DIVISION:

GURBIR S. GREWAL
ATTORNEY GENERAL OF NEW JERSEY

By: 
Lara J. Fogel
Deputy Attorney General
124 Halsey Street, 5th Floor
P.O. Box 45029
Newark, New Jersey 07101

Dated: 11/20/18, 2018

FOR RESPONDENTS:

By: 
Debra M. Lightner
Senior Vice President and Chief Compliance Officer
EmblemHealth
55 Water Street
New York, New York 10041

Dated: 11/8/18, 2018