

CONSUMER PROTECTION DIVISION
OFFICE OF THE ATTORNEY GENERAL
OF MARYLAND,
200 St. Paul Place
Baltimore, MD 21202,

Plaintiff,

v.

INMEDIATA HEALTH GROUP, LLC
AND INMEDIATA TECHNOLOGIES,
LLC,
636 Ave., San Patricio, San Juan, PR 00920,

Defendants.

IN THE
CIRCUIT COURT
FOR
BALTIMORE COUNTY

Case No. _____

COMPLAINT FOR PERMANENT INJUNCTION AND OTHER RELIEF

Plaintiff, the Consumer Protection Division of the Office of the Attorney General of Maryland (the “Division” or the “Plaintiff”), brings this action against Defendants Inmediata Health Group, LLC, and Inmediata Technologies, LLC (collectively, “Inmediata” or “Defendants”), for violating the Maryland Consumer Protection Act, Md. Code Ann., Com. Law §§ 13-101–13-501 (2013 Repl. Vol. and 2022 Supp.) (the “Consumer Protection Act”) and the Maryland Personal Information Protection Act, Md. Code Ann., Com. Law § 14-3501–14-3508 (2013 Repl. Vol and 2022 Supp.) (“Personal Information Protection Act”) stemming from a data breach exposing the personal information of approximately 1.5 million individuals between May 16, 2016 and January 15, 2019. In support thereof, Plaintiff states the following:

I. THE PARTIES

1. The Plaintiff is the Consumer Protection Division of the Office of the Attorney General of Maryland. The Division is charged with, among other things, enforcing and seeking redress for violations of Maryland’s consumer protection laws, including the Consumer Protection Act and the Personal Information Protection Act.

2. Defendant Inmediata Health Group, LLC is a limited liability corporation incorporated in the Commonwealth of Puerto Rico. Its principal office is located at 636 Avenue, San Patricio, San Juan, PR 00920, and a branch known as Inmediata Health Group Corp., is located at 200 South Tryon Street, Suite 1700, Charlotte, NC 28202.

3. Defendant Inmediata Technologies, LLC is a limited liability corporation incorporated in the Commonwealth of Puerto Rico. Its principal office is located at 636 Ave San Patricio, San Juan, PR 00920.

II. JURISDICTION AND VENUE

4. This Court has jurisdiction over the subject matter of this action and jurisdiction over the parties to this action, and venue is proper in this Court pursuant to Md. Code Ann., Cts. & Jud. Proc. §§ 6-103 and 6-201 (2013 Repl. Vol. and 2022 Supp.). At all times relevant to this Complaint, Inmediata has transacted business within the State of Maryland, including, but not limited to, in Baltimore County, by providing health care clearinghouse services to health care providers in Maryland. Inmediata was also in possession of the personal information of Maryland residents.

5. The Defendant agrees to waive notice as required by Md. Code Ann., Com. Law § 13-406 (2013 Repl. Vol. and 2022 Supp.).

III. BACKGROUND

6. Inmediata acts as a health care clearinghouse, facilitating financial and clinical transactions between health care providers and insurers across the United States.

7. In the regular course of business, Inmediata collects and maintains the personal information of individuals, including names, addresses, dates of birth, and Social Security numbers.

8. Inmediata also receives, uses, and maintains electronic Protected Health Information (“ePHI”) subject to the requirements 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 (“HIPAA”).

9. HIPAA and its rules require the implementation of appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of ePHI. *See* 45 CFR Part 160 and Subparts A and C of Part 164.

IV. STATEMENT OF FACTS

10. On January 15, 2019, the U.S. Department of Health & Human Services’ Office of Civil Rights (“OCR”) alerted Inmediata that the personal information held and maintained by Inmediata was exposed online.

11. Inmediata’s investigation revealed that beginning on May 16, 2016 two webpages were indexed by Bing Bot (a search engine web crawler), exposing the personal information of approximately 1.5 million individuals. The indexed webpages continued to be available through January 15, 2019.

12. Inmediata failed to prevent or discover Bing Bot crawling on the exposed webpages despite the availability of robots.txt Search Engine Optimization (“SEO”), a known information security measure.

13. Robots.txt, also known as the robots exclusion standard or protocol, is a text file located in the root or main directory of a website, which serves as an instruction for SEO spiders on which parts of a website they can and cannot crawl. Robots.txt files can be customized to expressly disallow access to particular webpages.

14. Inmediata admits that robots.txt scripting was not implemented until after the data breach. Further, Inmediata did not have practices in place to detect Bing Bot crawling on sensitive webpages.

15. In addition, HIPAA security risk assessments conducted by a third-party vendor from August 2017 to February 2019 flagged many “high risk” security deficiencies in Inmediata’s systems relating to account management, access controls, end-of-life practices, antivirus and firewall protection, encryption, segmentation, scanning, vendor management, intrusion detection and prevention, and logging and monitoring.

16. Among the security deficiencies identified were risks that Inmediata knew or should have known about, including among others, failures to implement its policies and procedures. For example, while Inmediata’s password policy set forth requirements for length and complexity, the assessment reflected that these requirements were not actually implemented.

17. Despite these data security failures, Inmediata boasted on its website that it provides “[i]ndustry leading security with our data safely stored in the cloud” and that it is “[c]ompliant with HIPAA, CMS, and ONC requirements.”

18. Inmediata also made promises to clients that it would take appropriate steps to protect personal information from unauthorized disclosure, which Inmediata failed to do.

19. Furthermore, although OCR notified Inmediata of the data breach on January 15, 2019, Inmediata did not begin mailing direct notice letters to impacted consumers until over three months later, on April 22, 2019.

20. Inmediata’s response to the data breach was disorganized and resulted in misaddressed notifications being sent to impacted consumers. This resulted not only in further impermissible disclosures of PHI in some cases, but also a substantial likelihood that certain impacted consumers never received proper, direct notice of the breach.

21. Inmediata's notices also failed to provide sufficient details or context as to why Inmediata possessed consumers' data, which may have caused recipients to dismiss the notices as illegitimate.

COUNT I
Violation of the Consumer Protection Act

22. The Plaintiff incorporates paragraphs 1 through 22 as if fully set forth herein.

23. The Defendants' practices, as set forth above, constitute unfair or deceptive trade practices in the sale and offer for sale of consumer services in violation of the Consumer Protection Act.

24. The Defendants' false and misleading statements regarding its data protection practices had the capacity, tendency, or effect of deceiving or misleading consumers and, pursuant to § 13-301(1) of the Consumer Protection Act, constitute unfair or deceptive trade practices that are prohibited by § 13-303 of the Consumer Protection Act.

25. The Defendants' failure to adequately inform consumers regarding its data protection practices constitutes a failure to state material facts, the omission of which has deceived or tended to deceive consumers and constitutes unfair or deceptive trade practices as defined in § 13-301(3) of the Consumer Protection Act that are prohibited by § 13-303 of the Consumer Protection Act.

26. The Defendants' practice of failing to take reasonable steps to protect consumers' personal information and the resulting data breach caused substantial harm to consumers, that consumers could not reasonably avoid, and which did not benefit the marketplace or competition, making it an unfair trade practice pursuant to § 13-303 of the Consumer Protection Act.

COUNT II
Violations of Personal Information Protection Act

27. The Division alleges paragraphs 1 through 22 as if fully set forth herein.

28. The Defendants collect, own, maintain and/or license the personal information of consumers residing in Maryland.

29. The Defendants have violated the Maryland Personal Information Protection Act by failing to implement and maintain reasonable security measures to protect records that contain personal information concerning Maryland consumers from unauthorized access, use, modification, or disclosure.

30. The Defendants' failure to take reasonable steps to protect consumers' personal information constitutes a violation of the Maryland Personal Information Protection Act and, pursuant to § 14-3508 of the Maryland Personal Information Protection Act, constitutes an unfair or deceptive trade practices and subjects the Defendants to the enforcement and penalty provisions contained in the Consumer Protection Act.

COUNT III
Violation of the Personal Information Protection Act

31. The Division alleges paragraphs 1 through 22 as if fully set forth herein.

32. The Defendants collect, own, maintain and/or license the personal information of consumers residing in Maryland.

33. The Defendants did not begin mailing direct notice letters to affected Maryland residents until April 22, 2019, ninety-seven (97) days after OCR alerted Inmediata of the data breach.

34. The Defendants knew or should have known that the data breach was reasonably likely to result in the misuse of personal information, and subject to the notification provisions §§ 14-3504(b)(2) and (c)(2).

35. The Defendants were required to disclose the data breach to affected Maryland consumers of the breach "as soon as reasonably practicable," but pursuant to § 14-3504(b)(3) and

(c)(3) of the Maryland Personal Information Protection Act, not later than forty-five (45) days after discovering or being notified of the breach.

36. The Defendants' delay in notifying Maryland residents was not permitted under § 14-3504(d)(1) because it was not necessary to restore the integrity of a computer system, to discover the scope of the breach, or in response to a law enforcement request.

37. The Defendants violated the Maryland Personal Information Protection Act by failing to notify consumers of the breach impacting their personal information within the forty-five (45) day time period required by § 14-3504(b)(3) and (c)(3) of the Maryland Personal Information Protection Act, and, pursuant to § 14-3508 of the Maryland Personal Information Protection Act, constitutes an unfair or deceptive trade practices and subjects the Defendants to the enforcement and penalty provisions contained in the Consumer Protection Act.

VI. PRAYER FOR RELIEF

WHEREFORE, the Plaintiff respectfully requests that the Court enter and Order and Judgment:

- (a) Requiring the Defendants to cease and desist from engaging in unfair or deceptive trade practices in violation of the Maryland Consumer Protection Act and Personal Information Protection Act;
- (b) Requiring the Defendants to take affirmative action, including the payment of restitution to consumers;
- (c) Requiring the Defendants to pay economic damages;
- (d) Requiring the Defendants to pay the costs of this proceeding, including all costs of investigation;
- (e) Requiring the Defendants to pay a suitable civil penalty pursuant to §13-410 of

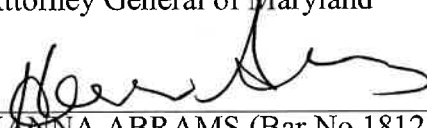
the Consumer Protection Act; and

- (f) Granting such other and further relief as is appropriate and necessary.

Respectfully submitted,

ANTHONY G. BROWN
Attorney General of Maryland

By:


HANNA ABRAMS (Bar No.1812120121)
Assistant Attorney General
Consumer Protection Division
Office of the Attorney General of Maryland
200 St. Paul Place, 16th Floor
Baltimore, MD 21202
(410) 576-7296
habrams@oag.state.md.us

Attorney for Plaintiff

Dated: 10/17/23

CONSUMER PROTECTION DIVISION
OFFICE OF THE ATTORNEY GENERAL
OF MARYLAND,
200 St. Paul Place
Baltimore, MD 21202,

Plaintiff,

v.

INMEDIATA HEALTH GROUP, LLC,
AND INMEDIATA TECHNOLOGIES,
LLC,

Defendants.

IN THE
CIRCUIT COURT
FOR
BALTIMORE COUNTY

C-03-CV-23-004171

Case No. _____

FINAL JUDGMENT AND CONSENT DECREE

Plaintiff, the Consumer Protection Division of the Office of the Attorney General of Maryland (the "Division" or the "Plaintiff"), appearing through Attorney General Anthony G. Brown, and Defendants Inmediata Health Group, LLC, and Inmediata Technologies, LLC, including all of their subsidiaries, affiliates, agents, representatives, employees, successors, and assigns ("Defendants" together with the Division, the "Parties"), have agreed to the stipulations and terms of this Final Judgment and Consent Decree ("Judgment") without admission of any facts or liability of any kind as alleged in the Complaint, and with all Parties having waived their right to appeal, and the court having considered the matter and good cause appearing:

IT IS HEREBY ORDERED, ADJUDGED, AND DECREED THAT:

This Judgment resolves the Plaintiff's investigation of the data breach described in the Complaint regarding Defendants' compliance with the State unfair or deceptive acts and practices law ("Consumer Protection Law") and personal information protection act ("Personal Information Protection Law"), as well the federal 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 (“HIPAA”) (collectively, the “Relevant Laws”).

I. THE PARTIES

1. Plaintiff is the Consumer Protection Division of the Office of the Attorney General. The Consumer Protection Division is responsible for enforcement of Maryland’s consumer protection laws, including the Maryland Consumer Protection Act, Md. Code Ann., Com. Law §§ 13-101 through 13-501 (2013 Repl. Vol. and 2022 Supp.) and Maryland Personal Information Protection Act, Md. Code Ann., Com. Law §§ 14-3501 through 14-3508 (2013 Repl. Vol. and 2022 Supp.). Plaintiff, pursuant to 42 U.S.C. § 1320d-5(d), may also enforce HIPAA.

2. Defendant Inmediata Health Group, LLC is a limited liability corporation incorporated in the Commonwealth of Puerto Rico. Its principal office is located at 636 Avenue, San Patricio, San Juan, PR 00920, and a branch known as Inmediata Health Group Corp., is located at 200 South Tryon Street, Suite 1700, Charlotte, NC 28202.

3. Defendant Inmediata Technologies, LLC is a limited liability corporation incorporated in the Commonwealth of Puerto Rico. Its principal office is located at 636 Ave San Patricio, San Juan, PR 00920.

II. BACKGROUND

4. On January 15, 2019, the U.S. Department of Health & Human Services’ Office of Civil Rights alerted Defendants that the electronic protected health information (“ePHI”) held and maintained by the Defendants was exposed online. Defendants’ investigation revealed that a coding issue allowed two webpages to be indexed by Bing Bots from May 16, 2016 and continuing through January 15, 2019, potentially exposing the ePHI of approximately 1.5 million U.S.

individuals.

5. The Attorneys General of Alabama, Arizona, Arkansas, Colorado, Connecticut, Delaware, Georgia, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Montana, Nebraska, New Hampshire, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, Puerto Rico, Rhode Island, South Carolina, Tennessee, Utah, Washington, West Virginia, and Wisconsin (collectively, the “Attorneys General”) investigated this incident pursuant to the Relevant Laws. Defendants are entering into a Judgment with each of the Attorneys General and each Attorney General’s Judgment incorporates the substantive terms included herein. To the extent there are differences, those arise from the requirements of local rules and state laws.

III. STIPULATIONS

6. Plaintiff and Defendants agree to and do not contest the entry of this Judgment.

7. At all times relevant to this matter, Defendants were engaged in trade and commerce affecting consumers in the State insofar as Defendants provided health care clearinghouse services to health care providers in the State. Defendants were also in possession of the Personal Information of Maryland residents.

8. At all times relevant to this matter, Defendants were Covered Entities subject to the requirements of HIPAA in that they acted as a health care clearinghouse, which facilitates financial and clinical transactions between health care providers and insurers across the United States.

9. Defendants consent to jurisdiction and venue in this Court for purposes of entry of this Judgment as well as for the purpose of any subsequent action to enforce it.

IV. JURISDICTION

10. Defendants, at all relevant times, have transacted business in Maryland, including, but not limited to, Baltimore County.

11. This Judgment is entered pursuant to and subject to Md. Code Ann., Com. Law § 13-402 (2013 Repl. Vol. and 2022 Supp.).

12. The Court finds that it has jurisdiction over Defendants for purposes of entry of this Judgment as well as for the purpose of any subsequent action to enforce it.

13. The Court finds that it has jurisdiction over the subject matter and over the Parties for the purpose of entering and enforcing this Judgment, and venue is proper in this Court pursuant to Md. Code Ann., Cts. & Jud. Proc. § 6-103 (2013 Repl. Vol. and 2022 Supp.). Further, the Court retains jurisdiction for the purpose of enabling the Parties to later apply to the Court for such further orders and relief as may be necessary for the construction, enforcement, execution or satisfaction of this Judgment.

V. DEFINITIONS

14. “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 that information.

15. “Business Associate” shall be defined in accordance with 45 C.F.R. § 160.103 and is a person or entity that provides certain services to or performs functions on behalf of covered entities, or other business associates of covered entities, that require access to Protected Health Information.

16. “Consumer Protection Law” shall mean the Maryland Consumer Protection Act, Md. Code Ann., Com. Law §§ 13-101 through 13-501 (2013 Repl. Vol. and 2022 Supp.).

17. “Covered Entity” shall be defined in accordance with 45 C.F.R. § 160.103 and is a health care clearinghouse, health plan, or health care provider that transmits health information in electronic form in connection with a transaction for which the U.S. Department of Health and Human Services has adopted standards.

18. “Data Breach” shall mean the unauthorized access to electronic protected health information (“ePHI”) that the Defendants held and maintained on two internal webpages which were indexed by Bing Bots occurring from May 16, 2016 and continuing through January 15, 2019, potentially exposing the sensitive PI and PHI of approximately 1.5 million U.S. individuals.

19. “Effective Date” shall be December 1, 2023.

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

21. “Encrypt” or “Encryption” shall mean to render unreadable, indecipherable, or unusable to an unauthorized person through a security technology or methodology accepted generally in the field of information security.

22. “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 or Business Associate, a Covered Entity or Business Associate 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 in 45 C.F.R. § 164.502(b) and § 164.514(d).

23. “Personal Information” or “PI” shall have the same definition as set forth in Md.

Code Ann., Com. Law § 14-3501 (2013 Repl. Vol. and 2022 Supp.).

24. “Personal Information Protection Law” shall mean the Maryland Personal Information Protection Act, Md. Code Ann., Com. Law §§ 14-3501 through 14-3508 (2013 Repl. Vol. and 2022 Supp.).

25. “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 or Business Associate that performs certain services on behalf of the Covered Entity, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E.

26. “Protected Health Information” or “PHI” shall be defined in accordance with 45 C.F.R. § 160.103.

27. “Security Incident” shall be synonymous with “Intrusion” and shall be defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system in accordance with 45 C.F.R. § 164.304.

28. “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 or Business Associate that performs certain services on behalf of the Covered Entity, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and C.

29. “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.

VI. INJUNCTIVE PROVISIONS

WHEREFORE, TO PROTECT CONSUMERS AND ENSURE FUTURE COMPLIANCE WITH THE LAW:

Compliance with State and Federal Laws

30. Defendants shall comply with the Consumer Protection Law and Personal Information Protection Law in connection with their collection, maintenance, and safeguarding of PI, PHI, and ePHI.

31. Defendants shall not make any representation that has the capacity, tendency, or effect of deceiving or misleading consumers in connection with the safeguarding of PI, PHI, or ePHI.

32. Defendants shall comply with the HIPAA Privacy and Security Rules and shall implement all Administrative and Technical Safeguards required by HIPAA.

Information Security Program

33. Defendants shall develop, implement, and maintain an information security program (“Information Security Program” or “Program”) that shall be written and shall contain administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of Defendants’ operations; (ii) the nature and scope of Defendants’ activities; and (iii) the sensitivity of the personal information that Defendants maintain. At a minimum, the Program shall include the information security requirements in Paragraphs 40 through 56 below.

34. Defendants shall design and update the Program consistent with the Minimum Necessary Standard to collect and/or maintain PHI only to the extent necessary to accomplish its intended purpose and to fulfill its regulatory, legal, and contractual obligations.

35. Each Defendant shall designate an executive or officer whose full-time responsibility will be to implement, maintain, and monitor the Program (hereinafter referred to as

the “Chief Information Security Officer” or “CISO”). The CISO shall have appropriate training, expertise, and experience to oversee the Program and shall regularly report to the Board of Directors (“Board”) and Chief Executive Officer (“CEO”) regarding the status of the Program, the security risks faced by the Defendant, resources required for implementation of the Program, and the security implications of Defendant’s business decisions. At a minimum, the CISO shall report to the Board and CEO any future Security Incident within forty-eight (48) hours of discovery, and shall also provide a regular written report to the Board on a quarterly basis and to the CEO on a monthly basis.

36. Defendants shall develop a written incident response plan (“Plan”) to prepare for and respond to any future Security Incidents. At a minimum, this plan shall provide for the following phases: Preparation; Detection and Analysis; Containment; Notification and Coordination with Law Enforcement; Eradication; Recovery; Consumer and Regulator Notification and Remediation; and Post-Incident Analysis. As part of the Plan, Defendants shall maintain specific policies and procedures requiring the review and approval of Consumer Notification letters and mailings before they are sent, which at a minimum:

- a. Ensure that Consumer Notification letters are drafted clearly and provide enough detail to enable consumers to understand why they are receiving the notification and what categories of PI, PHI, and/or ePHI were compromised;
- b. Require review of Consumer Notifications mailings prior to sending to ensure that addresses are accurate; and
- c. Require that consumers’ addresses are run through the National Change of Address database prior to mailing out Consumer Notifications.

37. Within ninety (90) days of the Effective Date, and at least annually thereafter,

Defendants shall provide data security and privacy training to all personnel with access to PI, PHI, or ePHI. Defendants shall provide this training to any employees newly hired to, or transitioned into, a role with access to PI, PHI, or ePHI, within thirty (30) days of hire or transition. Such training shall be appropriate to employees' job responsibilities and functions. Defendants shall document the trainings and the date(s) upon which they were provided.

38. Defendants may satisfy the requirements to implement and maintain the Program through review, maintenance, and as necessary, updating of an existing information security program and related safeguards, provided that such program and safeguards meet the requirements of this Judgment.

39. Defendants shall provide the resources and support necessary to fully implement the Program so that it functions as required and intended by this Judgment.

Specific Information Security Safeguards

40. **Code Review:** Defendants shall perform regular review of coding to ensure that PI, PHI, or ePHI is not indexed or indexable on externally facing webpages owned, controlled, licensed, or maintained by the Defendants or on the Defendants' behalf.

41. **Crawling Controls:** Defendants shall expressly disallow crawling of webpages owned, controlled, licensed, or maintained by the Defendants or on the Defendants' behalf by any bots, such as BingBot, containing PI, PHI, or ePHI.

42. **Password Management:** Defendants shall implement and maintain password policies and procedures requiring the use of strong, complex passwords, and ensuring that stored passwords are protected from unauthorized access.

43. **Account Management:** Defendants shall implement and maintain policies and procedures to manage, and limit access to and use of, all accounts with access to PI, PHI, or ePHI,

including individual accounts, administrator accounts, service accounts, and vendor accounts. In particular, Defendants shall appropriately limit the creation of new accounts in their system to protect against the creation of unauthorized accounts.

44. **Access Controls:** Defendants shall implement and maintain policies and procedures to ensure that access to PI, PHI, and ePHI is granted under the principle of least privilege. Such policies and procedures shall further include a means to regularly review access and access levels of users and remove network and remote access within twenty-four (24) hours of notification of termination for any employee whose employment has ended. Defendants shall require in any contract with a vendor that vendors also include a means to regularly review access and access level of users and remote network and remote access within twenty-four (24) hours of termination of any vendor, employee of the vendor, or anyone working on behalf of the vendor.

45. **Multi-Factor Authentication:** Defendants shall require the use of multi-factor authentication for remote access to systems(s) that store or permit access to PI or ePHI. Such multi-factor authentication methods should not include telephone or SMS-based authentication methods, but can include mobile applications, physical security keys, or other more secure options.

46. **Software Updates:** Defendants shall maintain, keep updated, and support software on their network.

47. **Antivirus:** Defendants shall implement and maintain current, up-to-date antivirus protection programs or a reasonably equivalent technology.

48. **Firewalls:** Defendants shall implement and maintain firewall policies and procedures to restrict connections between internal networks through appropriately configured hardware and software tools.

49. **Encryption:** Defendants shall Encrypt PI and ePHI at rest and in transit as

appropriate, and in accordance with applicable law.

50. **Segmentation:** Defendants shall implement, and maintain policies and procedures designed to appropriately segment its network, which shall, at a minimum, ensure that systems communicate with each other only to the extent necessary to perform their business and/or operational functions.

51. **Logging and Monitoring:** Defendants shall implement and maintain a Security Incident and Event Monitoring solution to detect and respond to malicious attacks. Defendants shall ensure that logs of system activity are regularly and actively reviewed and analyzed in as close to real-time as possible, and that appropriate follow-up and remediation steps are taken with respect to any Security Incident. Defendants shall further ensure that logs are protected from unauthorized access, destruction, and/or deletion.

52. **Intrusion Detection and Data Loss Prevention:** Defendants shall implement and maintain an intrusion detection and data loss prevention technology to detect and prevent unauthorized access and data exfiltration.

53. **Vulnerability Scanning:** Defendants shall conduct regular vulnerability scanning using industry-standard tool and shall take appropriate steps to remediate identified vulnerabilities.

54. **Risk Assessments:** Defendants shall obtain an annual risk assessment by a qualified, independent third party, which shall, at a minimum, include: the identification of internal and external risks to the security, confidentiality, or integrity of PI, PHI, and ePHI that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information; an assessment of the safeguards in place to control these risks; the evaluation and adjustment of the Program considering the results of the assessment, including the implementation of reasonable safeguards to control these risks; and documentation of safeguards implemented in

response to such annual risk assessments. Defendants shall retain documentation of the risk assessments and remedial measures for five (5) years and shall provide them to the Plaintiff upon request.

55. **Penetration Testing:** Defendants shall implement and maintain a risk-based penetration testing program reasonably designed to identify, assess, and remediate potential security vulnerabilities. Such testing shall occur on at least a biannual basis and shall include penetration testing of Defendants' internal and external network defenses. Defendants shall review the results of such testing, take steps to remediate findings revealed by such testing, and document such remediation. Defendants shall retain documentation of the penetration test results and remedial measures for five (5) years and shall provide them to the Plaintiff upon request.

56. **Business Associates:** Defendants shall develop, implement, and maintain written policies and procedures related to Business Associates, which at a minimum:

- a. Designate one or more individual(s) who are responsible for ensuring that Defendants enter into a Business Associate agreement with each of its Business Associates, prior to disclosing PI, PHI, or ePHI to the Business Associates;
- b. Assess Defendants' current and future business relationships to determine whether the relationship involves a Business Associate;
- c. Implement and maintain a process for negotiating and entering into Business Associate agreements with Business Associates prior to disclosing PI, PHI, or ePHI to the Business Associates; and
- d. Implement and maintain risk-based policies and procedures which limit disclosures of PI, PHI, or ePHI to the minimum amount necessary for the Business Associate to perform their duties.

Information Security Program Assessment

57. Defendants shall, within one hundred and eighty (180) days of the Effective Date, and thereafter annually for a period of five (5) years, submit to an assessment of their compliance with this Judgment, by an independent third-party assessor (“Assessor”). Following each such assessment, the Assessor shall prepare a report (“Security Report”) including its findings and recommendations, a copy of which shall be provided to the Indiana Attorney General within thirty days (30) of its completion.

58. Within ninety (90) days of their receipt of each Security Report, Defendants shall review and, to the extent necessary, revise their current policies and procedures based on the findings of the Security Report. Within one hundred eighty (180) days of Defendants’ receipt of each Security Report, Defendants shall forward to the Indiana Attorney General a description of any action they take and, if no action is taken, a detailed description why no action is necessary, in response to each Security Report.

V. PAYMENT TO THE STATES

59. Defendants shall make a total payment to the Attorneys General collectively in the amount of One Million, Four Hundred Thousand Dollars (\$1,400,000), to be divided among the Attorneys General at their discretion. Seven Hundred Thousand Dollars (\$700,000) shall be due December 1, 2023, and Seven Hundred Thousand Dollars (\$700,000) shall be due December 1, 2025. Payment in two equal installments is expressly premised upon the truthfulness, accuracy, and completeness of Inmediata’s financial statement submitted to the States and representations of its inability to pay the amount in its entirety by December 1, 2023.

60. The amount apportioned to the Maryland Attorney General is to be paid by Defendants directly to the Maryland Attorney General in an amount designated by the Attorneys

General and communicated to the Defendants. Out of the total amount, the Defendants shall pay Thirteen Thousand and Sixty-Six Dollars (\$13,066.00) to Maryland by December 1, 2023, and Thirteen Thousand and Sixty-Six Dollars (\$13,066.00) to Maryland by December 1, 2025. The money received by the Attorney General pursuant to this section may be used, at the sole discretion of the Attorney General, for purposes that may include placement in any consumer protection law enforcement fund, including future consumer protection or privacy enforcement, consumer education, litigation or local consumer aid fund or revolving fund, used to defray the costs of the inquiry leading hereto, or may be used for any other public purpose permitted by state law.

VI. RELEASE

61. Following full payment of the amounts due by Defendants under this Judgment, Plaintiff shall release and discharge Defendants from all civil claims that the Plaintiff could have brought under the Consumer Protect Act, the Personal Information Protection Act, and HIPAA based on Defendants' conduct as set forth in the Complaint. Nothing contained in this paragraph shall be construed to limit the ability of the Plaintiff to enforce the obligations that Defendants or their officers, subsidiaries, affiliates, agents, representatives, employees, successors, and assigns have under this Judgment. Further, nothing in the Judgment shall be construed to create, waive, or limit any private right of action.

62. Notwithstanding any term of this Judgment, any and all of the following forms of liability are specifically reserved and excluded from the release in Paragraph 61 above as to any entity or person, including Defendants:

a. Any criminal liability that any person or entity, including Defendants, has or may have to the States.

b. Any civil liability or administrative liability that any person or entity,

including Defendants, has or may have to this State under any statute, regulation, or rule not expressly covered by the release in Paragraph 61 above, including but not limited to, any and all of the following claims: (i) state or federal antitrust violations; (ii) state or federal securities violations; (iii) state insurance law violations; or (iv) state or federal tax claims.

VII. CONSEQUENCES OF NONCOMPLIANCE

63. Defendants represent that they have fully read this Judgment and understand the legal consequences attendant to entering into this Judgment. Defendants understand that any violation of this Order may result in the Plaintiff seeking all available relief to enforce this Order, including an injunction, civil penalties, court and investigative costs, attorneys' fees, restitution, and any other relief provided by the laws of the State or authorized by a court. If the Plaintiff is required to file a petition to enforce any provision of this Judgment against one or more Defendants, the particular Defendant(s) involved in such petition agrees to pay all court costs and reasonable attorneys' fees associated with any successful petition to enforce any provision of this Judgment against such Defendant(s).

VIII. GENERAL PROVISIONS

64. Any failure of the Plaintiff to exercise any of its rights under this Judgment shall not constitute a waiver of any rights hereunder.

65. Defendants hereby acknowledge that their undersigned representative or representatives are authorized to enter into and execute this Judgment. Defendants are and have been represented by legal counsel and have been advised by their legal counsel of the meaning and legal effect of this Judgment.

66. This Judgment shall bind Defendants and their officers, subsidiaries, affiliates,

agents, representatives, employees, successors, future purchasers, acquiring parties, and assigns.

67. Defendants shall deliver a copy of this Judgment to, or otherwise fully apprise, their executive management having decision-making authority with respect to the subject matter of this Judgment within thirty (30) days of the Effective Date.

68. The settlement negotiations resulting in this Judgment have been undertaken by Defendants and the Plaintiff in good faith and for settlement purposes only, and no evidence of negotiations or communications underlying this Judgment shall be offered or received in evidence in any action or proceeding for any purpose.

69. Defendants waive notice and service of process for any necessary filing relating to this Judgment, and the Court retains jurisdiction over this Judgment and the Parties hereto for the purpose of enforcing and modifying this Judgment and for the purpose of granting such additional relief as may be necessary and appropriate. No modification of the terms of this Judgment shall be valid or binding unless made in writing, signed by the Parties, and approved by the Court in which the Judgment is filed, and then only to the extent specifically set forth in such Judgment.

70. Defendants do not object to *ex parte* submission and presentation of this Judgment by the Plaintiff to the Court, and do not object to the Court's approval of this Judgment and entry of this Judgment by the clerk of the Court.

71. The Parties agree that this Judgment does not constitute an approval by the Plaintiff of any of Defendants' past or future practices, and Defendants shall not make any representation to the contrary.

72. The requirements of the Judgment are in addition to, and not in lieu of, any other requirements of state or federal law. Nothing in this Judgment shall be construed as relieving Defendants of the obligation to comply with all local, state, and federal laws, regulations, or rules,

nor shall any of the provisions of the Judgment be deemed as permission for Defendants to engage in any acts or practices prohibited by such laws, regulations, or rules.

73. This Judgment shall not create a waiver or limit Defendants' legal rights, remedies, or defenses in any other action by the Plaintiff, except an action to enforce the terms of this Judgment or to demonstrate that Defendants were on notice as to the allegations contained herein.

74. This Judgment shall not waive Defendants' right to defend themselves, or make argument in, any other matter, claim, or suit, including, but not limited to, any investigation or litigation relating to the subject matter or terms of the Judgment, except with regard to an action by the Plaintiff to enforce the terms of this Judgment.

75. This Judgment shall not waive, release, or otherwise affect any claims, defenses, or position that Defendants may have in connection with any investigations, claims, or other matters not released in this Judgment.

76. Defendants shall not participate directly or indirectly in any activity to form or proceed as a separate entity or corporation for the purpose of engaging in acts prohibited in this Judgment or for any other purpose which would otherwise circumvent any part of this Judgment.

77. If any clause, provision, or section of this Judgment shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity, or unenforceability shall not affect any other clause, provision, or section of this Judgment and this Judgment shall be construed and enforced as if such illegal, invalid, or unenforceable clause, section, or other provision had not been contained herein.

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

79. To the extent that there are any, Defendants agree to pay all court costs associated with the filing of this Judgment.

IX. NOTICES UNDER THIS ORDER

80. Any notices or other documents required to be sent to the Parties pursuant to the Judgment shall be sent by (a) United States Mail, Certified Return Receipt Requested, or other nationally recognized courier service that provides tracking services and identification of the person signing for the documents; and (b) email, to the persons identified below at the addresses listed below, unless a different contact person or address is specified in writing by the party changing such contact person or address:

For the Plaintiff:

Hanna Abrams
Assistant Attorney General
Consumer Protection Division
200 St. Paul Place, 16th Floor
Baltimore, MD 21202
habrams@oag.state.md.us

With a copy to:

Chief
Consumer Protection Division
200 St. Paul Place, 16th Floor
Baltimore, MD 21202

For the Defendants:

Lindsay Nicle, Partner
Constangy, Brooks, Smith & Prophete, LLP
1201 Elm Street, Suite 2550
Dallas, TX
lnickle@constangy.com
Direct: 469.632.1679
Mobile: 806.535.0274

APPROVED:

DEFENDANT, INMEDIATA HEALTH GROUP, LLC

By:  _____

Date: 10/3/23

Severiano Lopez-Marrero
Founder, Chief Executive Officer
Inmediata Health Group LLC
636 Ave. San Patricio
San Juan, PR 00920
(787) 774-0606

DEFENDANT, INMEDIATA TECHNOLOGIES, LLC

By:  _____

Date: 10/3/23

Severiano Lopez-Marrero
Founder, Chief Executive Officer
Inmediata Technologies LLC
636 Ave. San Patricio
San Juan, PR 00920
(787) 774-0606

COUNSEL FOR DEFENDANTS

By: Jamie Seibert
Jamie Seibert, Attorney


Date: October 12, 2023

Maryland Bar No. 2112150102
Constangy, Brooks, Smith & Prophete, LLP
145 West Ostend Street, Suite 600
Baltimore, Maryland 21230
jseibert@constangy.com
Direct: 410.891.6080

Lindsay Nickle, Partner
Texas Bar No. 24007747
Constangy, Brooks, Smith & Prophete, LLP
1201 Elm Street, Suite 2550
Dallas, TX 75270
lnickle@constangy.com
Direct: 469.632.1679

APPROVED:

PLAINTIFF
ANTHONY G. BROWN
Attorney General of Maryland

By: 
Hanna Abrams (Bar No. 1812120121)
Assistant Attorney General
Consumer Protection Division
200 St. Paul Place, 16th Floor
Baltimore, MD 21202
(410) 576-7296
habrams@oag.state.md.us

Date: Oct. 17, 2023

SO ORDERED:

By: _____
Judge,
Circuit Court for Baltimore County

Date: _____