

1 Tina Wolfson, California Bar No. 174806

AHDOOT & WOLFSON, PC

10728 Lindbrook Drive

2 Los Angeles, CA 90024

Tel: (310) 474-9111

3 Fax: (310) 474-8585

twolfson@ahdootwolfson.com

4 Cornelius P. Dukelow, Oklahoma Bar No. 19086

ABINGTON COLE + ELLERY

320 South Boston Avenue

6 Suite 1130

Tulsa, Oklahoma 74103

7 918.588.3400 (*telephone & facsimile*)

cdukelow@abingtonlaw.com

8 Benjamin F. Johns, Pennsylvania Bar No. 201373

9 Andrew W. Ferich, Pennsylvania Bar No. 313696

CHIMICLES SCHWARTZ KRINER

& DONALDSON-SMITH LLP

10 One Haverford Centre

11 361 Lancaster Avenue

Haverford, Pennsylvania 19041

12 610.642.8500

bfj@chimicles.com

13 awf@chimicles.com

14 *Attorneys for Plaintiffs and the Proposed Classes*

15 **UNITED STATES DISTRICT COURT**
16 **FOR THE SOUTHERN DISTRICT OF CALIFORNIA**

17 VICKI STASI, SHANE WHITE, and
18 CRYSTAL GARCIA, individually and
19 on behalf of all others similarly situated,

20 Plaintiffs,

21 v.

22 INMEDIATA HEALTH GROUP
23 CORP.; and DOES 1 through 20,
24 inclusive,

25 Defendants.

Case No. '19CV2353 JM LL

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

1 Plaintiffs, Vicki Stasi, Shane White, and Crystal Garcia (“Plaintiffs”), on behalf
2 of themselves individually and on behalf of all others similarly situated, allege on
3 personal knowledge, investigation of counsel, and on information and belief as follows:

4 **BRIEF SUMMARY OF THE CASE**

5 1. In January of 2019, Inmediata Health Group Corp. (“Inmediata” or
6 “Defendant”) first learned that it was experiencing a large data security incident (the
7 “Inmediata Data Security Incident”) resulting in the exposure of personal information of
8 approximately 1,565,338 individuals (“Affected Individuals”).

9 2. Even though Inmediata was storing sensitive personal information that it
10 knew was valuable to criminals, and vulnerable to exfiltration, Inmediata failed to take
11 security precautions necessary to protect Affected Individuals’ data. Because Inmediata
12 failed to take necessary security precautions, Affected Individuals’ data was viewable
13 online and downloadable. Additionally, due to a webpage setting that permitted search
14 engines to index internal webpages that Inmediata uses for business operations,
15 Affected Individuals’ data was also searchable, findable, viewable, and downloadable
16 by anyone with access to an internet search engine such as Google, Yahoo, Bing, etc.

17 3. The Affected Individuals’ data exposed by Inmediata included the types of
18 information that federal and state law requires companies to take security measures to
19 protect: names, addresses, Social Security numbers, dates of birth, gender, and medical
20 claim information including dates of service, diagnosis codes, procedure codes and
21 treating physicians (“Personal Information”). This data should have received the most
22 rigorous protection available – it did not.

23 **PARTIES**

24 4. Plaintiff Vicki Stasi is an individual residing in Seminole, Florida.
25 Inmediata received and collected Ms. Stasi’s Personal Information, which Inmediata
26 maintained in its computer systems. At the end of April, 2019, Ms. Stasi received a
27 letter dated April 22, 2019, from Inmediata informing her that her Personal Information
28

1 may have been compromised as a result of the Inmediata Data Security Incident. Ms.
2 Stasi now engages in monthly monitoring of her credit reports and weekly monitoring
3 of her credit cards and bank accounts. Ms. Stasi also received an improperly addressed
4 letter for another individual affected by the Inmediata Data Security Incident – the
5 improperly addressed letter included Ms. Stasi’s address, but the name of an individual
6 not residing at Ms. Stasi’s address. Ms. Stasi has spent approximately 20 hours of her
7 own time attempting to determine how she is connected to Inmediata, how her
8 information came into the possession of Inmediata, and trying to make sure she has not
9 and does not become victimized because of the Inmediata Data Security Incident.

10 5. Plaintiff Shane White is an individual residing in Moorhead, Minnesota.
11 Inmediata received and collected Mr. White’s Personal Information, which Inmediata
12 maintained in its computer systems. In approximately late April of 2019, Mr. White
13 received a letter dated April 22, 2019, from Inmediata informing him that his Personal
14 Information may have been compromised as a result of the Inmediata Data Security
15 Incident. Mr. White has spent approximately 2 hours of his own time attempting to
16 determine how he is connected to Inmediata and how his information came into the
17 possession of Inmediata.

18 6. Plaintiff Crystal Garcia is an individual residing in Poway, California.
19 Inmediata received and collected Ms. Garcia’s Personal Information, which Inmediata
20 maintained in its computer systems. In April of 2019, Ms. Garcia received a letter dated
21 April 22, 2019, from Inmediata informing her that her Personal Information may have
22 been compromised as a result of the Inmediata Data Security Incident. After being
23 notified of the breach, Ms. Garcia placed credit freezes on her credit reports with the
24 three major U.S. consumer credit reporting agencies in order to detect potential identity
25 theft and fraudulent activity. Ms. Garcia now engages in monthly monitoring of her
26 credit and her bank accounts. As a result of the Inmediata Data Security Incident, Ms.
27 Garcia has spent her own money and numerous hours addressing issues arising from the
28 Inmediata Data Security Incident. Etc.

1 specialty types including medical, dental, allied health and ambulance. SecureClaim
2 supports billing for professional, dental, and institutional claims.

3 14. On or about April 24, 2019, Inmediata publicly admitted via a press release
4 that: “In January 2019, Inmediata became aware that some electronic health information
5 was viewable online due to a webpage setting that permitted search engines to index
6 internal webpages that are used for business operations.”

7 <https://portal.inmediata.com/patients-of-data-security-incident/> (last visited July 23,
8 2019).

9 15. In approximately April of 2019, Inmediata began filing with various state
10 Attorneys General sample “Notice of Data Security Incident” letters that mirrored the
11 language of the letters sent to individual consumers (including Plaintiffs). The
12 California sample letters are attached hereto as Exhibit A.

13 16. The notice explained that “[i]n January 2019, Inmediata became aware that
14 some of its member patients’ electronic patient health information was publicly
15 available online as a result of a webpage setting that permitted search engines to index
16 pages that are part of an internal website we use for our business operations.”

17 17. The notice further explained that “information potentially impacted by this
18 incident may have included your name, address, date of birth, gender, and medical
19 claim information including dates of service, diagnosis codes, procedure codes and
20 treating physician.”

21 18. Inmediata’s notice acknowledged the very real threat that the incident
22 would result in identity theft, fraud, and other similar risks by further informing
23 recipients of the notice—such as Plaintiffs—to “remain vigilant by reviewing your
24 account statements and credit reports closely.”

25 19. Inmediata’s notice also instructed victims to “promptly report any
26 fraudulent activity or any suspected incidence of identity theft to proper law
27 enforcement authorities, your state attorney general, and/or the Federal Trade
28 Commission (FTC).”

1 20. Notably, Inmediata did not and has not offered or provided to the victims
2 any fraud insurance to date. Furthermore, to date, Inmediata has only offered or
3 provided identity monitoring services to victims who had their Social Security Numbers
4 disclosed. Instead, Inmediata merely provided some victims with contact information
5 for Experian, Transunion, and Equifax as well as for the Federal Trade Commission-
6 Consumer Response Center. Inmediata made general suggestions to contact local
7 authorities and police, in addition to suggestions on implementing a credit freeze if
8 necessary. Essentially, all of these steps are mandated generalities used by virtually
9 every company when publishing alerts about data security breaches. Inmediata failed to
10 make any additional effort to mitigate or remediate the damage caused by its failure to
11 protect sensitive personal and medical information.

12 21. Inmediata’s own statements confirm that the Plaintiffs and the Class
13 Members are subject to continued, future risk of identity theft, fraudulent charges and
14 other damages. For instance, Inmediata warned consumers “remain vigilant by
15 reviewing your account statements and credit reports closely. If you detect any
16 suspicious activity on an account, you should promptly notify the financial institution or
17 company with which the account is maintained. You also should promptly report any
18 fraudulent activity or any suspected incidence of identity theft to proper law
19 enforcement authorities, your state attorney general, and/or the Federal Trade
20 Commission (FTC).”

21 22. A breach report filed with the Secretary of the U.S. Department of Health
22 and Human Services on May 7, 2019, states that 1,565,338 individuals were affected by
23 the Inmediata Data Security Incident. The May 7, 2019, filing characterizes the breach
24 type as an “unauthorized access/disclosure” and further indicates that the breached
25 information was located on a “network server”.

26 23. Although Inmediata knew of the Inmediata Data Security Incident no later
27 than January of 2019, Inmediata took no steps to notify patients whose information was
28 affected until April 22, 2019, when Inmediata began mailing notification letters to the

1 potentially affected individuals directly and until April 24, 2019, via a post on
2 Inmediata’s website.

3 24. Inmediata had obligations created by HIPAA, and based on industry
4 standards, to keep the compromised Personal Information confidential and to protect it
5 from unauthorized disclosures. Plaintiffs and Class Members provided their Personal
6 Information to Inmediata’s clients with the common sense understanding that
7 Inmediata’s clients and any business partners to whom Inmediata’s clients disclosed the
8 Personal Information (i.e., Inmediata) would comply with their obligations to keep such
9 information confidential and secure from unauthorized disclosures.

10 25. Inmediata acknowledges that it is subject to HIPAA. Inmediata states that
11 it provides “[i]ndustry leading security with our data safely stored in the cloud”, and
12 that it is “[c]ompliant with HIPAA, CMS and ONC requirements”.
13 <<https://portal.inmediata.com/about-us/>> (last visited July 23, 2019).

14 26. Inmediata’s data security obligations and promises were particularly
15 important given the substantial increase in data breaches — particularly those in the
16 healthcare industry — preceding January 2019, which were widely known to the public
17 and to anyone in Inmediata’s industries.

18 27. Inmediata’s security failures demonstrate that it failed to honor its duties
19 and promises by not:

20 a. Maintaining an adequate data security system to reduce the risk of
21 data leaks, data breaches, and cyber-attacks;

22 b. Adequately protecting Plaintiffs’ and Class Members’ Personal
23 Information;

24 c. Ensuring the confidentiality and integrity of electronic protected
25 health information it created, received, maintained, and/or transmitted, in violation of
26 45 C.F.R. § 164.306(a)(1);

27 d. Implementing technical policies and procedures for electronic
28 information systems that maintain electronic protected health information to allow

1 access only to those persons or software programs that have been granted access rights
2 in violation of 45 C.F.R. § 164.312(a)(1);

3 e. Implementing policies and procedures to prevent, detect, contain,
4 and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

5 f. Implementing procedures to review records of information system
6 activity regularly, such as audit logs, access reports, and security incident tracking
7 reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

8 g. Protecting against any reasonably anticipated threats or hazards to
9 the security or integrity of electronic protected health information in violation of 45
10 C.F.R. § 164.306(a)(2);

11 h. Protecting against reasonably anticipated uses or disclosures of
12 electronic protected health information that are not permitted under the privacy rules
13 regarding individually identifiable health information in violation of 45 C.F.R. §
14 164.306(a)(3);

15 i. Ensuring compliance with the HIPAA security standard rules by its
16 workforce in violation of 45 C.F.R. § 164.306(a)(4); and/or

17 j. Training all members of its workforce effectively on the policies and
18 procedures with respect to protected health information as necessary and appropriate for
19 the members of its workforce to carry out their functions and to maintain security of
20 protected health information, in violation of 45 C.F.R. § 164.530(b).

21 **It is Well Established That Data Breaches Lead to Identity Theft**

22 28. Plaintiffs and other Class Members have been injured by the disclosure of
23 their Personal Information in the Inmediata Data Security Incident.

24 29. The United States Government Accountability Office noted in a June 2007
25 report on Data Breaches (“GAO Report”) that identity thieves use identifying data such
26 as Social Security Numbers to open financial accounts, receive government benefits and
27
28

1 incur charges and credit in a person’s name.¹ As the GAO Report states, this type of
2 identity theft is the most harmful because it often takes some time for the victim to
3 become aware of the theft, and the theft can impact the victim’s credit rating adversely.

4 30. In addition, the GAO Report states that victims of identity theft will face
5 “substantial costs and inconveniences repairing damage to their credit records” and their
6 “good name.”²

7 31. Identity theft victims are frequently required to spend many hours and
8 large amounts of money repairing the impact to their credit. Identity thieves use stolen
9 personal information for a variety of crimes, including credit card fraud, phone or
10 utilities fraud, and bank/finance fraud.

11 32. There may be a time lag between when sensitive personal information is
12 stolen and when it is used. According to the GAO Report:

13 [L]aw enforcement officials told us that in some cases, *stolen data may be*
14 *held for up to a year or more before being used to commit identity theft.*
15 Further, once stolen data have been sold or posted on the Web, *fraudulent*
16 *use of that information may continue for years.* As a result, studies that
17 attempt to measure the harm resulting from data breaches cannot necessarily
rule out all future harm.³

18 33. With access to an individual’s Personal Information, criminals can do more
19 than just empty a victim’s bank account—they can also commit all manner of fraud,
20 including: obtaining a driver’s license or official identification card in the victim’s
21 name but with the thief’s picture; using the victim’s name and SSN to obtain
22 government benefits; or, filing a fraudulent tax return using the victim’s information. In
23

24 _____
25
26 ¹ See *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the*
Full Extent Is Unknown (June 2007), United States Government Accountability Office, available at
27 <<https://www.gao.gov/new.items/d07737.pdf>> (last visited July 23, 2019).

28 ² *Id.* at 2, 9.

³ *Id.* at 29 (emphasis added).

1 addition, identity thieves may obtain a job using the victim’s SSN, rent a house, or
2 receive medical services in the victim’s name, and may even give the victim’s personal
3 information to police during an arrest, resulting in an arrest warrant being issued in the
4 victim’s name.⁴

5 34. Personal Information is such a valuable commodity to identity thieves that
6 once the information has been compromised, criminals often trade the information on
7 the “cyber black-market” for years. As a result of recent large-scale data breaches,
8 identity thieves and cyber criminals have openly posted stolen credit card numbers,
9 SSNs, and other Personal Information directly on various Internet websites making the
10 information publicly available.

11 35. A study by Experian found that the “average total cost” of medical identity
12 theft is “about \$20,000” per incident, and that a majority of victims of medical identity
13 theft were forced to pay out-of-pocket costs for healthcare they did not receive in order
14 to restore coverage.⁵ Indeed, data breaches and identity theft have a crippling effect on
15 individuals and detrimentally impact the entire economy as a whole.

16 36. Medical databases are especially valuable to identity thieves. According to
17 a 2012 Nationwide Insurance report, “[a] stolen medical identity has a \$50 street value
18 – whereas a stolen social security number, on the other hand, only sells for \$1.”⁶ In
19 fact, the medical industry has experienced disproportionately higher instances of
20 computer theft than any other industry.

21 37. To date, Inmediata does not appear to be taking any measures to assist
22 many affected Plaintiffs and Class Members other than telling them to simply do the
23 following:

24 _____
25
26 ⁴ See Federal Trade Commission, *Warning Signs of Identity Theft*, available at <https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft> (last visited July 23, 2019).

27 ⁵ See Elinor Mills, Study: Medical identity theft is costly for victims, CNET (Mar. 3, 2010),
28 <<https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/>> (last visited July 23, 2019).

⁶ Study: Few Aware of Medical Identity Theft Risk, Claims Journal,
<http://www.claimsjournal.com/news/national/2012/06/14/208510.htm> (last visited July 23, 2019).

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- “remain vigilant”;
- “review[] your account statements regularly and credit reports closely”;
- “keep[] a close eye on your credit card activity”;
- “promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities”;
- obtain a copy of free credit reports;
- contact the FTC and/or the state Attorney General’s office;
- enact a security freeze on credit files; and
- create a fraud alert.

None of these recommendations, however, require Inmediata to expend any effort to protect Plaintiffs’ and Class Members’ Personal Information.

38. Inmediata’s failure to adequately protect Plaintiffs’ and Class Members’ Personal Information has resulted in Plaintiffs and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money—while Inmediata sits by and does nothing to assist those affected by the incident. Instead, as Inmediata’s letter indicates, it is putting the burden on the Plaintiffs and Class Members to discover possible fraudulent activity and identity theft.

CLASS ALLEGATIONS

39. Plaintiffs bring this class action lawsuit on behalf of themselves and the proposed Class Members under Rule 23 of the Federal Rules of Civil Procedure.

40. Plaintiffs seek certification of a Nationwide Class, a California Sub-Class, a Florida Sub-Class, and a Minnesota Sub-Class defined as follows:

Nationwide Class: All persons in the United States whose Personal Information was compromised as a result of the Inmediata Data Security Incident announced by Inmediata on or around April 24, 2019.

1 41. In the alternative to the Nationwide Class, Plaintiffs seek
2 certification of the following state classes:

3 California Sub-Class: All persons in the State of California
4 whose Personal Information was compromised as a result of the
5 Inmediata Data Security Incident announced by Inmediata on or
6 around April 24, 2019.

7 Florida Sub-Class: All persons in the State of Florida whose
8 Personal Information was compromised as a result of the
9 Inmediata Data Security Incident announced by Inmediata on or
around April 24, 2019.

10 Minnesota Sub-Class: All persons in the State of Minnesota
11 whose Personal Information was compromised as a result of the
12 Inmediata Data Security Incident announced by Inmediata on or
13 around April 24, 2019.

14 42. Specifically excluded from the Classes are Defendant and any entities in
15 which Defendant has a controlling interest, Defendant’s agents and employees, the
16 judge to whom this action is assigned, members of the judge’s staff, and the judge’s
17 immediate family.

18 43. **Numerosity**: Plaintiffs do not know the exact number of Class Members,
19 but believe the Classes comprise approximately 1.5 million individuals throughout the
20 United States. As such, Class Members are so numerous that joinder of all members is
21 impracticable.

22 44. **Commonality**: Common questions of law and fact exist and predominate
23 over any questions affecting only individual Class Members. The common questions
24 include:

- 25 a. Whether Defendant engaged in the conduct alleged herein;
- 26 b. Whether Defendant failed to adequately safeguard Plaintiffs’ and
27 Class Members’ Personal Information;

1 c. Whether Defendant failed to protect Plaintiffs’ and Class Members’
2 Personal Information properly and/or as promised;

3 d. Whether Defendant’s computer system and data security practices
4 used to protect Plaintiffs’ and the Class Members’ Personal Information violated
5 HIPAA, federal, state and local laws, or Defendant’s duties;

6 e. Whether Defendant engaged in unfair, unlawful, or deceptive
7 practices by failing to safeguard Plaintiffs’ and Class Members’ Personal Information;

8 f. Whether Defendant violated the consumer protection statutes, data
9 breach notification statutes, state unfair insurance practice statutes, state insurance
10 privacy statutes, and/or state medical privacy statutes applicable to Plaintiffs and Class
11 Members;

12 g. Whether Defendant failed to notify Plaintiffs and Class Members
13 about the Inmediata Data Security Incident as soon as practical and without delay after
14 the Inmediata Data Security Incident was discovered;

15 h. Whether Defendant acted negligently in failing to safeguard
16 Plaintiffs’ and Class Members’ Personal Information;

17 i. Whether Defendant express or implied contractual obligations to
18 protect the confidentiality of Plaintiffs’ and the Class Members’ Personal Information,
19 and to have reasonable data security measures;

20 j. Whether Defendant’s conduct described herein constitutes a breach
21 of contract with Plaintiffs and Class Members;

22 k. Whether Plaintiffs and Class Members are entitled to damages as a
23 result of Defendant’s wrongful conduct;

24 l. Whether Plaintiffs and Class Members are entitled to restitution as a
25 result of Defendant’s wrongful conduct;

26 m. What equitable relief is appropriate to redress Defendant’s wrongful
27 conduct; and
28

1 n. What injunctive relief is appropriate to redress the imminent and
2 currently ongoing harm faced by Plaintiffs and Class Members.

3 45. **Typicality:** Plaintiffs' claims are typical of the claims of the Class
4 Members. Plaintiffs and Class Members were injured through Defendant's uniform
5 misconduct and their legal claims arise from the same core practices of Defendant.

6 46. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the
7 interests of the Classes, and have retained counsel competent and experienced in
8 complex litigation and class actions. Plaintiffs have no interests antagonistic to those of
9 the Classes, and there are no defenses unique to Plaintiffs. Plaintiffs and their counsel
10 are committed to prosecuting this action vigorously on behalf of the members of the
11 proposed Classes, and have the financial resources to do so. Neither Plaintiffs nor their
12 counsel have any interest adverse to those of the other members of the Classes.

13 47. **Risks:** The proposed action meets the requirements of Fed. R. Civ. P. 23
14 because prosecution of separate actions by individual members of the Classes would
15 create a risk of inconsistent or varying adjudications that would establish incompatible
16 standards for Defendant or would be dispositive of the interests of members of the
17 proposed Classes. Furthermore, the Inmediata Database still exists, and is still
18 vulnerable to future attacks – one standard of conduct is needed to ensure the future
19 safety of the Inmediata Database.

20 48. **Injunctive Relief:** The proposed action meets the requirements of Fed. R.
21 Civ. P. 23(b)(2) because Defendant has acted or has refused to act on grounds generally
22 applicable to the Classes, so that final injunctive relief or corresponding declaratory
23 relief is appropriate as to the Classes as a whole.

24 49. **Predominance:** The proposed action meets the requirements of Fed. R.
25 Civ. P. 23(b)(3) because questions of law and fact common to the Classes predominate
26 over any questions that may affect only individual Class Members in the proposed
27 Classes.

1 **50. Superiority:** The proposed action also meets the requirements of Fed. R.
2 Civ. P. 23(b)(3) because a class action is superior to all other available methods of
3 fairly and efficiently adjudicating this dispute. The injury sustained by each Class
4 Member, while meaningful on an individual basis, is not of such magnitude that it is
5 economically feasible to prosecute individual actions against Defendant. Even if it were
6 economically feasible, requiring more than 1.5 million injured plaintiffs to file
7 individual suits would impose a crushing burden on the court system and almost
8 certainly lead to inconsistent judgments. By contrast, class treatment will present far
9 fewer management difficulties and provide the benefits of a single adjudication,
10 economies of scale, and comprehensive supervision by a single court. Plaintiffs
11 anticipate no unusual difficulties in managing this class action.

12 **51. Certification of Particular Issues:** In the alternative, this action may be
13 maintained as class action with respect to particular issues, in accordance with Fed. R.
14 Civ. P. 23(c)(4).

15 **52.** Finally, all members of the purposed Classes are readily ascertainable.
16 Defendant has access to addresses and other contact information for members of the
17 Classes, which can be used to identify Class Members.

18 **COUNT I**
19 **NEGLIGENCE**

20 **53.** Plaintiffs reallege and incorporate by reference every allegation set forth in
21 the preceding paragraphs as though alleged in this Count.

22 **54.** This count is brought on behalf of all Classes.

23 **55.** Inmediata collected and stored the Personal Information of Plaintiffs and
24 Class Members.

25 **56.** Inmediata knew, or should have known, of the risks inherent in collecting
26 and storing the Personal Information of Plaintiffs and Class Members.

27 **57.** Inmediata owed duties of care to Plaintiffs and Class Members whose
28 Personal Information had been entrusted with Inmediata.

1 58. Inmediata breached its duties to Plaintiffs and Class Members by failing to
2 provide fair, reasonable, or adequate computer systems and data security practices to
3 safeguard Plaintiffs’ and Class Members’ Personal Information.

4 59. Inmediata acted with wanton disregard for the security of Plaintiffs’ and
5 Class Members’ Personal Information. Inmediata knew or should have known that it
6 had inadequate computer systems and data security practices to safeguard such
7 information, and Inmediata knew or should have known that hackers were attempting to
8 access the Personal Information in health care databases, such as theirs.

9 60. A “special relationship” exists between Inmediata and the Plaintiffs and
10 Class Members. Inmediata entered into a “special relationship” with Plaintiffs and Class
11 Members by placing their Personal Information in the Inmediata Database –
12 information that Plaintiffs and Class Members had been required to provide to
13 Inmediata.

14 61. But for Inmediata’s wrongful and negligent breach of its duties owed to
15 Plaintiffs and Class Members, Plaintiffs and Class Members would not have been
16 injured.

17 62. The injury and harm suffered by Plaintiffs and Class Members was the
18 reasonably foreseeable result of Inmediata’s breach of its duties. Inmediata knew or
19 should have known that it was failing to meet its duties, and that Inmediata’s breach
20 would cause Plaintiffs and Class Members to experience the foreseeable harms
21 associated with the exposure of their Personal Information.

22 63. As a direct and proximate result of Inmediata’s negligent conduct,
23 Plaintiffs and Class Members now face an increased risk of future harm.

24 64. As a direct and proximate result of Inmediata’s negligent conduct,
25 Plaintiffs and Class Members have suffered injury and are entitled to damages in an
26 amount to be proven at trial.

COUNT II

NEGLIGENCE PER SE

1
2
3 65. Plaintiffs reallege and incorporate by reference every allegation set forth in
4 the preceding paragraphs as though alleged in this Count.

5 66. This count is brought on behalf of all Classes.

6 67. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Inmediata
7 had a duty to provide fair and adequate computer systems and data security practices to
8 safeguard Plaintiffs’ and Class Members’ Personal Information.

9 68. Pursuant to HIPAA (42 U.S.C. § 1302d et. seq.), Inmediata had a duty to
10 implement reasonable safeguards to protect Plaintiffs’ and Class Members’ Personal
11 Information.

12 69. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Inmediata
13 had a duty to protect the security and confidentiality of Plaintiffs’ and Class Members’
14 Personal Information.

15 70. Pursuant to Fla. Stat. § 501.171(2), Cal. Civ. Code § 56 et seq., and Minn.
16 Stat. §144.291 et seq., Inmediata had a duty to implement and maintain reasonable
17 security procedures and practices to safeguard Plaintiffs’ and Class Members’ Personal
18 Information.

19 71. Inmediata breached its duties to Plaintiffs and Class Members under the
20 Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d et. seq.),
21 Gramm- Leach-Bliley Act (15 U.S.C. § 6801), Fla. Stat. § 501.171(2), Cal. Civ. Code §
22 56 et seq., and Minn. Stat. §144.291 et seq. by failing to provide fair, reasonable, or
23 adequate computer systems and data security practices to safeguard Plaintiffs’ and Class
24 Members’ Personal Information.

25 72. Inmediata’s failure to comply with applicable laws and regulations
26 constitutes negligence *per se*.

1 73. But for Inmediata’s wrongful and negligent breach of its duties owed to
2 Plaintiffs and Class Members, Plaintiffs and Class Members would not have been
3 injured.

4 74. The injury and harm suffered by Plaintiffs and Class Members was the
5 reasonably foreseeable result of Inmediata’s breach of its duties. Inmediata knew or
6 should have known that it was failing to meet its duties, and that Inmediata’s breach
7 would cause Plaintiffs and Class Members to experience the foreseeable harms
8 associated with the exposure of their Personal Information.

9 75. As a direct and proximate result of Inmediata’s negligent conduct,
10 Plaintiffs and Class Members now face an increased risk of future harm.

11 76. As a direct and proximate result of Inmediata’s negligent conduct,
12 Plaintiffs and Class Members have suffered injury and are entitled to damages in an
13 amount to be proven at trial.

14 **COUNT III**

15 **BREACH OF CONTRACTS TO WHICH PLAINTIFFS AND CLASS**
16 **MEMBERS WERE INTENDED THIRD-PARTY BENEFICIARIES**

17 77. Plaintiffs reallege and incorporate by reference every allegation set forth in
18 the preceding paragraphs as though alleged in this Count.

19 78. Upon information and belief, Plaintiffs and Class Members are intended
20 third-party beneficiaries of contracts entered into between Inmediata and its customers,
21 including health plans, hospitals, IPAs, and independent physicians.

22 79. Upon further information and belief, these contracts and require, inter alia,
23 that Inmediata take appropriate steps to safeguard the sensitive Personal Information
24 entrusted to it by its customers that obtain that information from Plaintiffs and Class
25 Members.

26 80. Plaintiffs and the Class Members are intended third party beneficiaries of
27 these contracts. Under the circumstances, recognition of a right to performance by
28 Plaintiffs and the Class Members is appropriate to effectuate the intentions of the parties

1 to these contracts. One or more of the parties to these contracts intended to give
2 Plaintiffs and the Class Members the benefit of the performance promised in the
3 contracts.

4 81. Inmediata breached these agreements, which directly and/or proximately
5 caused Plaintiffs and the Class Members to suffer substantial damages.

6 82. Upon further information and belief, Inmediata saved (or avoided
7 spending) a substantial sum of money by knowingly failing to comply with its
8 contractual obligations, and continues to do so.

9 83. Accordingly, Plaintiffs and Class Members who have been injured are
10 entitled to damages, restitution, and other relief in an amount to be proven at trial.

11 **COUNT IV**

12 **VIOLATION OF CALIFORNIA’S**

13 **CONFIDENTIALITY OF MEDICAL INFORMATION ACT**

14 **Cal. Civ. Code § 56 et seq.**

15 84. Plaintiffs reallege and incorporate by reference every allegation set forth in
16 the preceding paragraphs as though alleged in this Count.

17 85. This count is brought on behalf of the California Sub-Class.

18 86. Inmediata is a “Contractor” as defined by Cal. Civ. Code § 56.05(d) and/or
19 a “Provider of Health Care” as expressed in Cal. Civ. Code § 56.06.

20 87. Plaintiffs and Class Members are “Patients” as defined by Cal. Civ. Code §
21 56.05(k).

22 88. The Plaintiffs’ and Class Members’ Personal Information that was the
23 subject of the Inmediata Data Security Incident included “Medical Information” as
24 defined by Cal. Civ. Code § 56.05(j).

25 89. In violation of California’s Confidentiality of Medical Information Act,
26 Inmediata disclosed Medical Information of Plaintiffs and Class Members without first
27 obtaining an authorization.

1 90. In violation of California’s Confidentiality of Medical Information Act,
2 Inmediata intentionally shared, sold, used for marketing, or otherwise used Medical
3 Information of Plaintiffs and Class Members for a purpose not necessary to provide
4 health care services to Plaintiffs or Class Members.

5 91. In violation of California’s Confidentiality of Medical Information Act,
6 Inmediata further disclosed Medical Information regarding Plaintiffs and Class
7 Members to persons or entities not engaged in providing direct health care services to
8 Plaintiffs or Class Members or their providers of health care or health care service plans
9 or insurers or self-insured employers.

10 92. In violation of California’s Confidentiality of Medical Information Act,
11 Inmediata created, maintained, preserved, stored, abandoned, destroyed, or disposed of
12 Medical Information of Plaintiffs and Class Members in a manner that did not preserve
13 the confidentiality of the information contained therein.

14 93. In violation of California’s Confidentiality of Medical Information Act,
15 Inmediata negligently created, maintained, preserved, stored, abandoned, destroyed, or
16 disposed of Medical Information of Plaintiffs and Class Members.

17 94. In violation of California’s Confidentiality of Medical Information Act,
18 Inmediata’s electronic health record systems or electronic medical record systems did
19 not protect and preserve the integrity of Plaintiffs’ and Class Members’ Medical
20 Information.

21 95. In violation of California’s Confidentiality of Medical Information Act,
22 Inmediata negligently released confidential information and records of Plaintiffs and
23 Class Members.

24 96. In violation of California’s Confidentiality of Medical Information Act,
25 Inmediata negligently disclosed Medical Information of Plaintiffs and Class Members.

26 97. In violation of California’s Confidentiality of Medical Information Act,
27 Inmediata knowingly and willfully obtained, disclosed, and/or used Medical
28 Information of Plaintiffs and Class Members.

1 98. As a direct and proximate result of Inmediata’s violation of Cal. Civ. Code
2 § 56 *et seq.*, Plaintiffs and Class Members now face an increased risk of future harm.

3 99. As a direct and proximate result of Inmediata’s violation of Cal. Civ. Code
4 § 56 *et seq.*, Plaintiffs and Class Members have suffered injury and are entitled to
5 damages in an amount to be proven at trial.

6 **COUNT V**

7 **VIOLATION OF THE MINNESOTA HEALTH RECORDS ACT**

8 **Minn. Stat. § 144.291 *et seq.***

9 100. Plaintiffs reallege and incorporate by reference every allegation set forth in
10 the preceding paragraphs as though alleged in this Count.

11 101. This count is brought on behalf of the Minnesota Sub-Class.

12 102. Inmediata is a “Patient Information Service” as defined by Minn. Stat. §
13 144.291(Sub-2)(h), a “Provider” as defined by Minn. Stat. § 144.291(Sub-2)(i), and/or a
14 “Related Health Care Entity” as defined by Minn. Stat. § 144.291(Sub-2)(k).

15 103. Plaintiffs and Class Members are “Patients” as defined by Minn. Stat. §
16 144.291(Sub-2)(g).

17 104. The Plaintiffs’ and Class Members’ Personal Information that was the
18 subject of the Inmediata Data Security Incident included “Health Records” as defined
19 by Minn. Stat. § 144.291(Sub-2)(c).

20 105. The Plaintiffs’ and Class Members’ Personal Information that was the
21 subject of the Inmediata Data Security Incident included “Identifying Information” as
22 defined by Minn. Stat. § 144.291(Sub-2)(d).

23 106. The Plaintiffs’ and Class Members’ Personal Information that was the
24 subject of the Inmediata Data Security Incident included information in an “Individually
25 Identifiable Form” as defined by Minn. Stat. § 144.291(Sub-2)(e).

26 107. In violation of the Minnesota Health Records Act, Inmediata released
27 Health Records of Plaintiffs and Class Members without first obtaining consent or
28 authorization.

1 108. In violation of the Minnesota Health Records Act, Inmediata negligently or
2 intentionally released Health Records of Plaintiffs and Class Members.

3 109. As a direct and proximate result of Inmediata's violation of Minn. Stat.
4 §144.291 *et seq.*, Plaintiffs and Class Members now face an increased risk of future
5 harm.

6 110. As a direct and proximate result of Inmediata's violation of Minn. Stat.
7 §144.291 *et seq.*, Plaintiffs and Class Members have suffered injury and are entitled to
8 damages in an amount to be proven at trial.

9 **PRAYER FOR RELIEF**

10 Plaintiffs, on behalf of themselves and the Classes, respectfully request the Court
11 order relief and enter judgment in their favor and against Inmediata as follows:

12 A. An order certifying this action as a class action under Fed. R. Civ. P. 23,
13 defining the Classes as requested herein, appointing the undersigned as Class counsel,
14 and finding that Plaintiffs are proper representatives of the Classes requested herein.

15 B. Plaintiffs request injunctive and other equitable relief as is necessary to
16 protect the interests of the Classes, including (i) an order prohibiting Inmediata from
17 engaging in the wrongful and unlawful acts described herein; (ii) requiring Inmediata to
18 protect all data collected or received through the course of their business in accordance
19 with HIPAA regulations, the Gramm-Leach Bliley Act, other federal, state and local
20 laws, and best practices under industry standards; (iii) requiring Inmediata to design,
21 maintain, and test their computer systems to ensure that Personal Information in their
22 possession is adequately secured and protected; (iv) requiring Inmediata to disclose any
23 future data breaches in a timely and accurate manner; (v) requiring Inmediata to engage
24 third-party security auditors as well as internal security personnel to conduct testing,
25 including simulated attacks, penetration tests, and audits on Inmediata's systems on a
26 periodic basis and ordering them to promptly correct any problems or issues detected by
27 these auditors; (vi) requiring Inmediata to audit, test, and train their security personnel
28 to run automated security monitoring, aggregating, filtering and reporting on log

1 information in a unified manner; (vii) requiring Inmediata to implement multi-factor
2 authentication requirements; (viii) requiring Inmediata's employees to change their
3 passwords on a timely and regular basis, consistent with best practices; (ix) requiring
4 Inmediata to encrypt all Personal Information; (x) requiring Inmediata to audit, test, and
5 train its security personnel regarding any new or modified procedures; (xi) requiring
6 Inmediata to segment data by, among other things, creating firewalls and access
7 controls so that if one area of Inmediata's network is compromised, hackers cannot gain
8 access to other portions of Inmediata's systems; (xii) requiring Inmediata to purge,
9 delete, and destroy in a reasonably secure and timely manner Personal Information no
10 longer necessary for their provision of services; (xiii) requiring Inmediata to conduct
11 regular database scanning and securing checks; (xiv) requiring Inmediata to routinely
12 and continually conduct internal training and education to inform internal security
13 personnel how to identify and contain a breach when it occurs and what to do in
14 response to a breach; (xv) requiring Inmediata to provide lifetime credit monitoring and
15 identity theft repair services to Class Members; and (xvi) requiring Inmediata to educate
16 all Class Members about the threats they face as a result of the loss of their Personal
17 Information to third parties, as well as steps Class Members must take to protect
18 themselves.

19 C. A judgment awarding Plaintiffs and Class Members appropriate monetary
20 relief, including actual damages, punitive damages, treble damages, statutory damages,
21 exemplary damages, equitable relief, restitution, and disgorgement;

22 D. An order that Inmediata pay the costs involved in notifying the Class
23 Members about the judgment and administering the claims process;

24 E. Pre-judgment and post-judgment interest;

25 F. Attorneys' fees, expenses, and the costs of this action; and

26 G. All other and further relief as this Court deems necessary, just, and proper.
27
28

JURY DEMAND

Plaintiffs demand a trial by jury on all issues so triable.

DATED: December 9, 2019

Respectfully submitted,

/s/ Tina Wolfson

Tina Wolfson

AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, CA 90024
Tel: 310.474.9111
Fax: 310.474.8585
twolfson@ahdootwolfson.com

and

Cornelius P. Dukelow*
Oklahoma Bar No. 19086
ABINGTON COLE + ELLERY
320 South Boston Avenue
Suite 1130
Tulsa, Oklahoma 74103
918.588.3400 (*telephone & facsimile*)
cdukelow@abingtonlaw.com

and

Benjamin F. Johns*
Pennsylvania Bar No. 201373
Andrew W. Ferich*
Pennsylvania Bar No. 313696
CHIMICLES SCHWARTZ KRINER
& DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, Pennsylvania 19041
610.642.8500
bfj@chimicles.com
awf@chimicles.com

**Pro Hac Vice* application to be submitted

Counsel to Plaintiffs and the Proposed Classes

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

VICKI STASI, SHANE WHITE, and CRYSTAL GARCIA, individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff Pinellas (EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number) Tina Wolfson, AHDOOT & WOLFSON, PC 10728 Lindbrook Drive Los Angeles, CA 90024 T: 310-474-9111; F: 310-474-8585; E: twolfson@ahdootwolfson.com

DEFENDANTS

INMEDIATA HEALTH GROUP CORP.; and DOES 1 through 20, inclusive

County of Residence of First Listed Defendant (IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

'19CV2353 JM LL

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff, 2 U.S. Government Defendant, 3 Federal Question (U.S. Government Not a Party), 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

Table with columns for Plaintiff (PTF) and Defendant (DEF) citizenship and business location (Citizen of This State, Citizen of Another State, Citizen or Subject of a Foreign Country, Incorporated or Principal Place of Business In This State, Incorporated and Principal Place of Business In Another State, Foreign Nation).

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Large table with categories: CONTRACT, REAL PROPERTY, CIVIL RIGHTS, PRISONER PETITIONS, TORTS, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES.

V. ORIGIN (Place an "X" in One Box Only)

- 1 Original Proceeding, 2 Removed from State Court, 3 Remanded from Appellate Court, 4 Reinstated or Reopened, 5 Transferred from Another District (specify), 6 Multidistrict Litigation - Transfer, 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity): 28 U.S.C. § 1332(d); 28 U.S.C. §1332(d)(2)(A)
Brief description of cause: Negligence, Negligence Per Se, Breach of Contract, Violation of CA's Confidentiality of Medical Information Act.

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P. DEMAND \$ 5,000,000.00 CHECK YES only if demanded in complaint: JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE DOCKET NUMBER

DATE 12/09/2019 SIGNATURE OF ATTORNEY OF RECORD /s/ Tina Wolfson

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
- (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
- United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
- United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
- Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
- Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.
- Original Proceedings. (1) Cases which originate in the United States district courts.
- Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
- Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
- Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
- Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
- Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
- Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
- PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7.** Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
- Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
- Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

EXHIBIT A



April 22, 2019

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Data Security Incident

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

I am writing on behalf of Inmediata Health Group, Corp., (Inmediata) to inform you of a data security incident that may have resulted in the potential disclosure of your personal and medical information. At Inmediata, we take the security of all patient information very seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains information about steps you can take to protect your information and resources we are making available to you.

What Happened?

In January 2019, Inmediata became aware that some of its member patients' electronic patient health information was publicly available online as a result of a webpage setting that permitted search engines to index pages that are part of an internal website we use for our business operations. When we became aware of the incident, we immediately deactivated the website and engaged an independent computer forensics firm to assist us. Based on the investigation, we have no evidence that any files were copied or saved. In addition, we have not discovered any evidence that any information that may be involved in this incident has been misused. However, out of an abundance of caution, we are informing you about the incident and providing you with information and resources to assist you.

What information was involved?

The information potentially impacted by this incident may have included your name, address, date of birth, gender, and medical claim information including dates of service, diagnosis codes, procedure codes and treating physician. Please note that neither your Social Security number nor your financial information is involved in this incident.

What We Are Doing.

As soon as we learned about the incident, we took the steps described above. In addition, we are providing you with information about steps you can take to help protect your personal information. Also, we have taken steps to remove any indexed information from public search engines, and we are conducting system-wide assessments to ensure that our system and the information we store is secure.

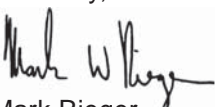
What You Can Do.

As stated above, while we are not aware of the misuse of any information potentially involved in this incident, you can follow the recommendations included with this letter to protect your personal information.

For more information.

We sincerely regret any inconvenience or concern that this matter may cause you and remain dedicated to protecting all information in our systems. Please do not hesitate to call 1-833-389-2392, Monday through Friday, 9:00 a.m. to 6:30 p.m. Eastern Time if you have questions about this event.

Sincerely,


Mark Rieger
CEO
Inmediata

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

TransUnion	Experian	Equifax	Free Annual Report
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov , and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>.



April 22, 2019

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Data Security Incident

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

I am writing on behalf of Inmediata Health Group, Corp., (Inmediata) to inform you of a data security incident that may have resulted in the potential disclosure of your personal and medical information. At Inmediata, we take the security of all patient information very seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains information about steps you can take to protect yourself and resources we are making available to you.

What Happened?

In January 2019, Inmediata became aware that some individuals' electronic patient health information was available online because of a webpage setting that permitted search engines to index pages that are part of an internal website we use for our business operations. When we became aware of the incident, we immediately deactivated the website and engaged an independent computer forensics firm to assist us. Based on the investigation, we have no evidence that any files were copied or saved. In addition, we have discovered no evidence that any information that may be involved in this incident has been misused. However, out of an abundance of caution, we are informing you about the incident and providing you with information and resources to assist you.

What information was involved?

The information potentially impacted by this incident may have included your name, address, Social Security number, date of birth, gender, and medical claim information, including dates of service, diagnosis codes, procedure codes and treating physician. Please note that your financial information is not involved in this incident.

What We Are Doing.

As soon as we learned about the incident, we took the steps described above. In addition, we are providing you with information about steps you can take to help protect your personal information. We also have taken steps to remove any indexed information from public search engines, and we are conducting system-wide assessments to ensure that our system and the information we store is secure.

What You Can Do.

While we do not believe any patient personal information was at risk, you can follow the recommendations included with this letter to protect your personal information. In addition, as a precautionary measure to safeguard your information from potential misuse, we are offering identity monitoring services for one year at no cost to you through Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit my.idmonitoringservice.com to activate and take advantage of your identity monitoring services.

*You have until **July 31, 2019** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

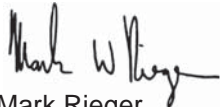
To receive credit services by mail instead of online, please call 1-833-389-2392. Additional information describing your services is included with this letter.

If you have questions or concerns about possible fraud, please call 1-833-389-2392, Monday through Friday, 9:00 a.m. to 6:30 p.m. Eastern Time.

For more information.

We sincerely regret any inconvenience or concern that this matter may cause you and remain dedicated to protecting all information in our systems. Please do not hesitate to call 1-833-389-2392, Monday through Friday, 9:00 a.m. to 6:30 p.m. Eastern Time if you have questions about this event.

Sincerely,

A handwritten signature in black ink, appearing to read "Mark Rieger", is positioned above the typed name.

Mark Rieger
CEO
Inmediata

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

TransUnion	Experian	Equifax	Free Annual Report
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov , and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Class Action Filed in Wake of January 2019 Inmediata Health Group Data Breach](#)
