



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 Chester, PA 19016 1-877-322-8228 www.transunion.com	P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 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 Washington, DC 20580 consumer.ftc.gov , and www.ftc.gov/idtheft 1-877-438-4338	200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 401-274-4400

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>.