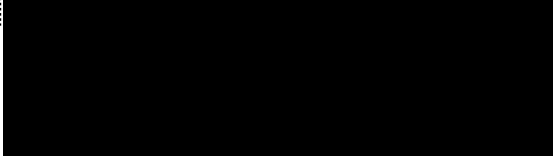




January 7, 2020



Subject: Notice of Data Security Incident

Dear [REDACTED],

I am writing to inform you of a data security incident experienced by PIH Health that may have involved some of your personal information and/or protected health information, described below. At PIH Health, we take the privacy and security of all information very seriously. That is why I am writing to inform you of this incident, to offer information about steps that can be taken to help protect your information, and to provide you with information about complimentary identity monitoring services that are being made available to you through Kroll, a global leader in risk mitigation and response. I sincerely apologize for any concern that this incident may cause you.

What happened? On June 18, 2019, PIH Health learned that certain PIH Health employee email accounts had potentially been accessed without authorization as a result of a targeted email phishing campaign. After learning of this information, PIH Health reset the passwords required to access the affected employee email accounts and implemented additional email and network security measures. PIH Health also immediately began an investigation and, in so doing, engaged leading, independent cybersecurity experts for assistance. As a result of the independent investigation conducted thereby, PIH Health learned on October 2, 2019 that certain PIH Health employee email accounts were accessed without authorization between June 11, 2019 and June 18, 2019 as a result of the above-referenced phishing campaign.

Upon receipt of confirmation of unauthorized access to certain PIH Health employee email accounts, PIH Health engaged the same leading, independent cybersecurity experts to determine whether the accessed email accounts contained personal information and/or protected health information that may have been subject to unauthorized access as a result. On November 12, 2019, as a result of that review, PIH Health learned that your information was contained within the accessed email accounts. PIH Health then worked diligently to identify up-to-date address information for all potentially impacted individuals in order to provide notification.

Please note that the above-referenced unauthorized access was limited to PIH Health email accounts. PIH Health is not aware of any evidence indicating unauthorized access to other PIH Health information systems. Moreover, PIH Health is not aware of the misuse of any information contained within the email accounts accessed without authorization. Nonetheless, out of an abundance of caution, PIH Health is providing you with this notice.

What information was involved? Information contained within the impacted email accounts may have included your name in combination with your treatment/diagnosis, health insurance, claims, and billing information, doctor's name, medical record number, Medicare/Medicaid ID, patient account number, Social Security number, and/or driver's license number. As mentioned above, PIH Health is not aware of any evidence of your information being misused.

What are we doing? PIH Health takes the security of all information within its possession very seriously. As soon as PIH Health discovered this incident, PIH Health took the steps described above. In addition, PIH Health has taken steps to enhance the security of all information, including patient information, to help prevent similar incidents from occurring in the future. PIH Health is also offering you complimentary identity monitoring services through Kroll, experts in data breach and recovery services. Additional details regarding the complimentary services being offered to you are enclosed.

What you can do: You can follow the recommendations on the following page to help monitor your information. In addition, we recommend that you review your financial account statements and if you notice any suspicious activity, contact your financial institution. We also encourage you to contact Kroll with any questions and to enroll in the complimentary services being provided to you. Activation instructions and a description of the services being provided are included with this letter.

For More Information: Further information and resources regarding how to safeguard your information appear on the following pages. If you have questions or need assistance, please contact Kroll at 1-833-963-0527, Monday through Friday from 6:00 a.m. to 3:30 p.m. Pacific Time. Kroll representatives are fully versed on this incident and can answer any questions that you may have regarding how to safeguard your personal information.

Our relationship with our patients is our most valued asset. I want to personally express my deepest regret for any worry or inconvenience that this incident may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'Anup Patel', written in a cursive style.

Anup Patel
Vice President, Enterprise Risk Management
PIH Health

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 one (1) year. 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. There should be no charge to place a security freeze on your credit file. 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, and 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.

As referenced above, PIH Has secured the services of Kroll to provide identity monitoring services at no cost to you for one year. Kroll is a global leader in risk mitigation and response and the Kroll team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Services

Visit krollbreach.idMonitoringService.com to activate and take advantage of your identity monitoring services.

You have until **April 9, 2020** to activate your identity monitoring services.

Membership number: [REDACTED]

If you have questions, please call 1-833-963-0527, Monday through Friday from 6:00 a.m. to 3:30 p.m. Pacific Time.

Take Advantage of Your Services

You've been provided with access to the following services 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 Chrome, Firefox, Safari and Edge. 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.