

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

October 1, 2021

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

Premier Patient Health Care (“Premier”) is an Accountable Care Organization works with your Primary Care Physicians to improve clinical outcomes under the Medicare Shared Savings Program (MSSP). Premier would like to make you aware of an incident that resulted in the impermissible use of your information. We take the security and privacy of your information very seriously and deeply apologize for any inconvenience this may cause you.

What Happened

On April 30, 2021, we discovered evidence indicating that a former executive of Premier accessed our computer system after the termination of his employment, obtained and accessed a file that contained your health information. We have investigated this incident but have been unable to determine how the information was further handled or used after it was acquired. We are continuing to investigate the full extent of the breach. Accordingly, we are providing you this notice to help you protect your information.

What Information Was Involved

The file contained your full name, age, sex, race, county and state of residence, and ZIP Code. The file also included Medicare beneficiary information such as your Medicare eligibility period, spend information, and hierarchical condition category risk score.

What We Are Doing

We have reported this incident to the United States Department of Health and Human Services (HHS), will make additional reporting/disclosures or other agencies as required and, we are prepared to assist in any resultant investigation. Additionally, we are reviewing our policies and procedures to better help prevent incidents such as this from occurring in the future.

What is Premier Management Company

Premier Management Company runs and operates the ACO, Premier Patient Health Care and has a business associate agreement (BAA) with you Primary Care Physicians who are covered entities. You received this notice because Premier Patient Healthcare (“Premier”) collected your information as a part of its work with the PCP’s and the shared savings program.

What You Can Do

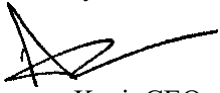
We have partnered with IDX to answer questions and provide valuable information about the incident. We encourage you to contact IDX with any questions by calling (833) 513-2613 or visiting <https://response.idx.us/premierpphc> for more information. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time.

While we are undertaking significant forensic investigations to investigate the breach, at this time, we do not have evidence indicating that your information has been further misused after it was acquired and accessed. However, we encourage you to remain vigilant and review the enclosed recommended steps document to learn general steps you may take to help protect your personal information. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have.

For More Information

If you have additional questions, please call (833) 513-2613.

Sincerely,

A handwritten signature in black ink, appearing to read 'Anwar Kazi', with a long horizontal stroke extending to the right.

Anwar Kazi, CEO
Premier Patient Health Care

(Enclosure)

Recommended Steps to help Protect your Information

Contact IDX at (833) 513-2613 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

2. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000

www.equifax.com

www.experian.com

www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

4. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.