PROVIDENCE
Health Plan
P.O. Box 4327
Portland, OR 97208-4327

ProvidenceHealthPlan.com

June 1, 2021

Bob Ferguson
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

Dear Mr. Ferguson:

Providence Health Plan ("PHP") offers health plans to Washington large group employers and individual market consumers pursuant to a Washington HCSC license. We also provide Oregon-regulated coverage to Oregon-domiciled employers, some of whom employ Washington residents. As required by WAC 284-04-625, I am writing to provide you notification of an event at Providence Health Plan / Providence Health Assurance that was flagged as a potential security risk for protected data.

The incident came to our attention on 4/16/2021 when a manager with Providence Health Plan was notified by an automated system that a temporary worker with access to data for our quality program attempted to send confidential information to their personal email address. On further investigation of the worker's email communications that day, we discovered the worker sent member protected health information to their personal email address in other messages that were successfully delivered, violating our security policies.

Our privacy and security team immediately responded to mitigate the incident, ensuring the worker's access privileges were terminated; conducting initial forensic analysis of the data in order to conclusively determine whether and to what extent documents forwarded by the worker were successfully delivered to their personal email address; coordination with the worker to agree to meet and attest to the deletion of sent emails containing confidential information. We also initiated a comprehensive data analysis review to assess the impact to members, including determining how the data mapped to lines of business and geographies. The investigation revealed the worker sent the first of several emails with member protected health information on 3/22/2021. Between that date and her last day on 4/16/2021, the worker sent several files containing PHI attributable to commercial members (fully insured and ASO), Medicare members, and one Medicaid member. The most significant file was a spreadsheet containing member protected health information used for quality program purposes. This spreadsheet listed member names, ID numbers, dates of birth, provider and clinic names used to assess health care performance requiring substantiation with clinical documentation, such as an immunization or diabetes measure. That data did not include SSN's or financial information.

PROVIDENCE
Health Plan

In total, emails reached the personal inbox with PHI attributable to approximately 5509 members across lines of business and geographies. The majority are Oregon-based residents and enrollees. Our analysis indicates 220 policyholders with with a Washington residence were affected.

While the worker was authorized to access this information in the course of their job duties, and we have engaged in the above-described mitigation activity that substantially reduced the likelihood that the data will be exploited, sending Providence Health Plan information unencrypted to a personal email address potentially compromised the security of the information. We have decided to treat this as a breach under HIPAA and abide by all of the associated notification requirements. We are in the process of preparing to meet the obligations under HIPAA to ensure affected members are individually notified in conjunction with notifying the Office for Civil Rights, local media where required by the HIPAA Privacy Rule, and applicable regulators. If you need to contact us regarding this matter, please contact me at Julie.Ebner@providence.org.

Sincerely,

Julie Ebner

Julie Ebner
Director, Compliance Services and Privacy
Privacy Officer for Providence Health Plan / Providence Health Assurance

PROVIDENCE Health Plan | PROVIDENCE Health Assurance

C/O IDX
<<Return Address>>
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:
(833) 406-2402
Or Visit:
https://response.idx.us/phpsecurity
Enrollment Code: <<XXXXXXXX>>

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

June 15, 2021

Notice of Data Breach

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

This letter is to notify you of a security incident involving your personal information.

What Happened

Providence Health Plan and Providence Health Assurance (Providence) hires temporary workers for short term tasks. On 4/16/2021, Providence's system prevented a temporary worker from sending an email containing protected health information to their personal email address. This prompted an investigation into the worker's previous emails where it was discovered that they had successfully sent protected health information to their personal email address on three previous occasions. While this worker was authorized to access your information in order to perform their job duties, they should not have sent the information to their personal email address.

What Information Was Involved

The document the workforce member emailed themselves was a tracking spreadsheet of certain quality performance measures. The information in the spreadsheet included your name, ID number, date of birth, health plan coverage type, provider and clinic name, and an abbreviation for which measurement Providence was reviewing, such as CBP for "Controlling High Blood Pressure," CDC for "Comprehensive Diabetes Care," and other similar measurements. **The spreadsheet did not contain your Social Security number or any financial information.**

What We Are Doing

On 4/18/2021, Providence met with the worker and witnessed them delete each email they sent themselves from their inbox and their deleted file. The worker signed a written statement that they did not save or share the information, or use it for non-work related purposes. The worker also stated that no other person had access to their personal email account.

The spreadsheet did not include financial information or Social Security numbers and therefore is unlikely to be used to exploit your credit. However, out of an abundance of caution, we are offering identity theft protection services through IDX. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. IDX is completely free to you and enrolling in this program will not hurt your credit score. With this protection, IDX will help you resolve issues if your identity is compromised. Please know that if this notice is regarding a minor or deceased loved one's information, credit monitoring may not be available due to a lack of an open credit history.

What You Can Do

Providence's designated point of contact for this breach is IDX. We encourage you to contact IDX with any questions and to enroll in free IDX services by calling (833) 406-2402, TTY/TDD 711, or by going to https://response.idx.us/phpsecurity and using the Enrollment Code provided above. IDX experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is September 15, 2021. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. **You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.**

Providence takes your privacy rights seriously and we regret any inconvenience or concern this may cause you.

Sincerely,

Providence Health Plan and Providence Health Assurance

(Enclosure)

Recommended Steps to Help Protect Your Information

1. **Website and Enrollment.** Go to or by going to https://response.idx.us/phpsecurity and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX membership. The monitoring included in the membership must be activated to be effective. Note: You must have open, established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact MyIDCare at (833) 406-2402, TTY/TDD 711, with your questions about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that, as a normal practice, 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.

If you discover any suspicious items and have enrolled in IDX, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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.

5. 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	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	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.

6. 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.

7. 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.

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

Washington Residents: Office of the Attorney General, 800 5th Ave., Suite 2000, Seattle, WA 98104-3188; www.atg.wa.gov; Telephone: 1-800-551-4636, TDD: 1-800-833-6388.

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.