Providence Health Plan
P.O. Box 4327
Portland, OR 97208-4327
www.ProvidenceHealthPlan.com

PROVIDENCE Health Plan

September 24, 2020

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. We provided notice to you on June 16, 2020 as required by WAC 284-04-625 due to a security incident involving protected information maintained by our business associate Zipari, in support of our Oregon small group line of business. We are providing an update about this previously reported security incident because Zipari has informed us that additional people were impacted by the same incident.

We previously reported that PHP utilizes a vendor named Zipari to provide certain functionality for the small group portion of the PHP producer portal related to enrollment documents. On 04/17/2020, Zipari attempted to notify PHP that as part of a security audit they discovered that two unauthorized parties had accessed unencrypted files containing PHP Oregon small group renewal documents. The files were placed in an Amazon Web Services "bucket" that had been incorrectly configured by Zipari to be publicly accessible. Upon learning of this, Zipari moved quickly to encrypt the folder containing the enrollment documents. The unauthorized access occurred in May, September, and November of 2019. Zipari represented their date of discovery to PHP as April 9, 2020.

Zipari continued to perform a forensic audit and subsequently discovered that additional information was accessed in the same incident. On July 28, 2020, Zipari notified PHP that additional files from late 2017 were also improperly accessed in May of 2019. Zipari and PHP have since worked to identify the affected members.

The data at issue was originally exchanged with Zipari for group enrollment purposes. PHP undertook a comprehensive review of the data that was accessible in the unsecured location and determined that it included member names and dates of birth. Certain information about the employer plans were also included, such as group numbers and employer names. The data did not contain health information, member ID numbers, social security numbers, or other sensitive financial information.

Providence Health Plan
P.O. Box 4327
Portland, OR 97208-4327
www.ProvidenceHealthPlan.com

PROVIDENCE Health Plan

PHP has been working since we received notification from Zipari on July 28, 2020 to obtain the requisite information to match affected member's names and dates of birth with ID numbers and addresses. PHP is preparing to meet its obligations under HIPAA to ensure this new group of members is notified via letter. We anticipate notifying the newly identified members on or before September 25, 2020.

Zipari's first report of the security incident led to the identification of 1,894 Washington residents on Oregon-regulated small group plans were included in the files. These members were notified of the security incident. Zipari's second report of additional affected individuals led to the identification of 1,430 Washington residents on Oregon-regulated small group plans that were affected by this security incident. Therefore, the total number of affected Washington residents is now 3,324. The substantial majority of affected members live in our core service area of Oregon.

If you have any questions or need further information regarding this incident, you may contact me at 503-574-5652 or by sending an email to: aaron.bals@providence.org

Sincerely,

Aaron Bals
Chief Compliance & Risk Officer
Privacy Officer

zipari

C/O ID Experts
PO Box 4600
Everett WA 98204

ENDORSE

NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY

BREAK

To Enroll, Please Call:
(833) 579-1105
Or Visit:
https://ide.myidcare.com/zipari-providence
Enrollment Code: <<XXXXXXXX>>

September 25, 2020

SEQ
CODE 2D
Ver 1A

Notice of Data Breach

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

Zipari is sending this letter to you, as a business associate (vendor) of Providence Health Plan, in order to notify you of a security incident involving your name and date of birth.

What Happened

As a business associate for Providence Health Plan, Zipari provides technology services related to the preparation of enrollment documents for your employer-sponsored Providence health plan.

Zipari discovered that a coding error had resulted in certain unencrypted Providence Health Plan enrollment documents being accessible to unauthorized individuals. The incident was discovered by Zipari as a result of a security scan. Upon discovery, Zipari took immediate action to investigate and remediate the incident.

As part of our investigation, Zipari conducted a detailed analysis to determine whether the documents containing personal information may have been improperly accessed. On April 9, 2020, we determined that certain Providence enrollment documents had been accessed by unauthorized IP addresses in May, September, and November of 2019. Zipari reached out to Providence Health Plan about the incident on April 17, 2020, and worked together with Providence Health Plan to ensure notification of impacted individuals.

Zipari also continued to perform a forensic audit and subsequently discovered that additional information was accessed in the same incident. On July 28, 2020, Zipari notified Providence Health Plan that additional files from late 2017 were also improperly accessed in May of 2019. Zipari and Providence Health Plan have since worked to match your name and date of birth with your address in order to send you notification of this incident.

What Information Was Involved

The enrollment documents included your name and date of birth, as well as the name and contact information of the employer-sponsor for your Providence health plan. No medical history or health information was included.

What We Are Doing

Zipari has encrypted the enrollment documents and taken additional action to secure these files. We have also remediated the coding error that led to the incident and have implemented further access controls to prevent unauthorized access to these files.

Although it is unlikely that your name and date of birth could lead to medical or financial fraud, out of an abundance of caution, we are offering you MyIDCare™ identity theft protection services through ID Experts®. MyIDCare includes:

12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. MyIDCare is completely free to you and enrolling in this program will not hurt your credit score. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What You Can Do

Providence Health Plan's designated point of contact for its members with respect to this breach is ID Experts. We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (833) 579-1105, TTY/TDD (866) 405-2133, or by going to https://ide.myidcare.com/zipari-providence and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 a.m. to 6 p.m. Pacific Time. Please note the deadline to enroll is December 25, 2020. MyIDCare representatives are knowledgeable about this incident and can answer questions or concerns you may have regarding protection of your personal information.

We encourage you to remain vigilant for incidents of fraud by monitoring your insurance statements and explanations of benefits. If you see services on your insurance statements or explanations of benefits that you did not receive, please call the customer service number on your member ID card. We also recommend that you monitor your financial account statements. If you see charges or activity you did not authorize, please contact your financial institution immediately.

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.

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

Sincerely,

Zipari

(Enclosure)

MyIDCare™

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://ide.myidcare.com/zipari-providence 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 MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at (833) 579-1105, TTY/TDD (866) 405-2133, 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 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 MyIDCare, notify them immediately by calling or by logging into the MyIDCare 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.

SEQ
CODE 2D

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.

Providence Health Plan
P.O. Box 4327
Portland, OR 97208-4327
www.ProvidenceHealthPlan.com

June 16, 2020

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. We are providing this notice to you as required by WAC 284-04-625 due to a security incident involving protected information maintained in support of our Oregon small group line of business.

PHP utilizes a vendor named Zipari to provide certain functionality for the small group portion of the PHP producer portal related to enrollment documents. On 04/17/2020, Zipari attempted to notify PHP that as part of a security audit they discovered that two unauthorized parties had accessed unencrypted files containing PHP Oregon small group renewal documents. The files were placed in an Amazon Web Services "bucket" that had been incorrectly configured by Zipari to be publicly accessible. Upon learning of this, Zipari moved quickly to encrypt the folder containing the enrollment documents. The unauthorized access occurred in May, September, and November of 2019. Zipari represented their date of discovery to PHP as April 9, 2020.

The data at issue was originally exchanged with Zipari for group enrollment purposes. PHP undertook a comprehensive review of the data that was accessible in the unsecured location and determined that it included member names and dates of birth. Certain information about the employer plans were also included, such as group numbers and employer names. The data did not contain health information, member ID numbers, social security numbers, or other sensitive financial information.

PHP has been working since the date we received notification from Zipari to obtain the requisite information to evaluate this matter and determine an appropriate response under applicable state and federal laws. PHP is preparing to meet its obligations under HIPAA to ensure members are individually notified via letter, to notify applicable regulators including the Office for Civil Rights, and to notify local media where required. We anticipate notifying members on or before June 20, 2020.

Providence Health Plan
P.O. Box 4327
Portland, OR 97208-4327
www.ProvidenceHealthPlan.com

Our analysis determined that 1,894 Washington residents on Oregon-regulated small group plans were included in the files and will therefore will be notified. The substantial majority of affected members live in our core service area of Oregon.

If you have any questions or need further information regarding this incident, you may contact me at 503-574-5652 or by sending an email to: aaron.bals@providence.org

Sincerely,

Aaron Bals
Chief Compliance & Risk Officer
Privacy Officer

zipari

C/O ID Experts
PO Box 4219
Everett WA 98204

ENDORSE

NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY

SEQ
CODE 2D
Ver 1A

BREAK

To Enroll, Please Call:
(833) 579-1105
Or Visit:
https://ide.myidcare.com/zipari-providence
Enrollment Code: <<XXXXXXXX>>

June 19, 2020

Notice of Data Breach

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

Zipari is sending this letter to you, as a business associate (vendor) of Providence Health Plan, in order to notify you of a security incident involving your name and date of birth.

What Happened

As a business associate for Providence Health Plan, Zipari provides technology services related to the preparation of enrollment documents for your employer-sponsored Providence health plan.

Zipari discovered that a coding error had resulted in certain unencrypted Providence Health Plan enrollment documents being accessible to unauthorized individuals. The incident was discovered by Zipari as a result of a security scan. Upon discovery, Zipari took immediate action to investigate and remediate the incident.

As part of our investigation, Zipari conducted a detailed analysis to determine whether the documents containing personal information may have been improperly accessed. On April 9, 2020, we determined that certain Providence Health Plan enrollment documents had been accessed by unauthorized IP addresses in May, September, and November of 2019. Zipari reached out to Providence Health Plan about the incident on April 17, 2020.

What Information Was Involved

The enrollment documents included your name and date of birth, as well as the name and contact information of the employer-sponsor for your Providence health plan. No medical history or health information was included.

What We Are Doing

Zipari has encrypted the enrollment documents and taken additional action to secure these files. We have also remediated the coding error that led to the incident and have implemented further access controls to prevent unauthorized access to these files.

Although it is unlikely that your name and date of birth could lead to medical or financial fraud, out of an abundance of caution, we are offering you MyIDCare™ identity theft protection services through ID Experts®. MyIDCare includes: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. MyIDCare is completely free to you and enrolling in

this program will not hurt your credit score. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What You Can Do

Providence Health Plan's designated point of contact for its members with respect to this breach is ID Experts. We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (833) 579-1105, TTY/TDD (866) 405-2133, or by going to https://ide.myidcare.com/zipari-providence and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 a.m. to 6 p.m. Pacific Time. Please note the deadline to enroll is September 19, 2020. MyIDCare representatives are knowledgeable about this incident and can answer questions or concerns you may have regarding protection of your personal information.

We encourage you to remain vigilant for incidents of fraud by monitoring your insurance statements and explanations of benefits. If you see services on your insurance statements or explanations of benefits that you did not receive, please call the customer service number on your member ID card. We also recommend that you monitor your financial account statements. If you see charges or activity you did not authorize, please contact your financial institution immediately.

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.

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

Sincerely,

Zipari

(Enclosure)

MyIDCare™

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://ide.myidcare.com/zipari-providence 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 MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at (833) 579-1105, TTY/TDD (866) 405-2133, 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 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 MyIDCare, notify them immediately by calling or by logging into the MyIDCare 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.

SEQ
CODE 2D

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.