

Select Health Website Notice

November 1, 2019 – Select Health Network (“Select Health”) provides a provider network to certain health plans and additional services to healthcare providers, and we are issuing notice of a recent event that may impact the privacy of personal information for current or former members of these plans or healthcare providers.

We recently concluded an investigation into unusual activity related to an employee email account. Upon learning of the suspicious activity, Select Health immediately took steps to secure the email account and began working with third-party forensic experts to determine the nature and scope of the incident. The investigation confirmed that the Select Health employee email account was accessed by an unknown actor from May 22, 2019 to June 13, 2019.

The investigation was unable to determine with forensic certainty what emails or attachments, if any, were accessed by the unauthorized actor. In an abundance of caution, we worked with experts to perform a comprehensive review of all information stored in the email account at the time of incident to confirm the identities of the individuals whose information may have been accessible to the unauthorized actor. On October 1, 2019, Select Health received the results of the third-party audit. We immediately began reviewing the results of the audit to determine the identities and contact information for potentially impacted individuals and contact information. On November 1, 2019, Select Health began notifying business partners and certain individuals about this incident.

The following types of information were present in the email account and accessible to the unknown actor, which may include: Name, Address, Date of Birth, Member ID Number, Treating/Referring Physician, Health Insurance Information, Medical History Information, Treatment Information, Treatment Cost Information, Health Insurance Policy Number, and Medical Record Number. For a limited number of individuals, Social Security number may have also been impacted. At this time, there is no evidence of any actual or attempted misuse of the information accessible within the email account. No financial account information was impacted as a result of this event.

We take this incident and the security of personal information seriously. Upon learning of this incident, we immediately took steps to secure the affected email account. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. While we are unaware of any misuse of any personal information contained within the impacted email account, individuals are encouraged to remain vigilant against incidents of identity theft by reviewing account statements and explanations of benefits for unusual activity and report any suspicious activity immediately to your insurance company, health care provider, or financial institution. As an added precaution, we are also offering complimentary access to 12 months of credit monitoring services to those individuals who may have had their Social Security number impacted by this event.

Members seeking additional information regarding this event can call our toll-free assistance line at 1-833-935-1364 Monday through Friday, during the hours of 9:00 a.m. to 9:00 p.m., Eastern Time. You may also write to the Select Health Network at P.O. Box 6249, South Bend, IN 46660.

Providers seeking additional information regarding this event can call our toll-free assistance line at 1-833-935-1354 Monday through Friday, during the hours of 9:00 a.m. to 9:00 p.m., Eastern Time. You may also write to the Select Health Network at P.O. Box 6249, South Bend, IN 46660.

Best Practices

While we are unaware of any misuse of the personal information in the impacted email account, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to

prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

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

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

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

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

To monitor for actual or attempted misuse of Social Security benefits, you can create an account at <https://www.socialsecurity.gov/myaccount>. If you see an error or attempted misuse of social security benefits, you can go to your local Social Security Office for assistance. Local offices can be found using the following office locator - <https://secure.ssa.gov/ICON/main.jsp>.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to

file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Maryland residents: The Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For 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 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_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.

For Rhode Island residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is one Rhode Island residents impacted by this incident.

For 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/>.