

October 11, 2019 – Monterey Health Center recently became aware of an event that may have impacted the privacy of personal information relating to certain current and former patients. While Monterey Health Center is unaware of any attempted or actual misuse of personal information in relation to the event, it is providing potentially affected individuals with notice of the event, its response, and steps individuals may take to better protect against the possibility of identity theft and fraud, should they feel it is necessary to do so.

What Happened? On August 12, 2019, Monterey Health Center became aware that its electronic medical records system became encrypted due to “ransomware” deployed by an unknown actor. Because the server that was encrypted stored patient medical records, Monterey Health Center worked quickly to (1) restore access to the patient information so it could continue to care for patients without disruption and (2) investigate what happened and whether this incident resulted in any unauthorized access to, or theft of, patient information by the unknown actor.

Working with a third-party vendor Monterey Health Center was able to successfully restore the data contained on the impacted server. The forensic investigator also confirmed there was no exfiltration of data. Unfortunately, after an extensive investigation, Monterey Health Center was unable to determine whether this incident resulted in unauthorized access to patient information. Although Monterey Health Center has no indication that any patient information was viewed or stolen by an unauthorized actor, it is notifying potentially affected individuals about this incident in an abundance of caution due to the uncertain nature of the incident.

What Information Was Involved? The impacted server contained patient medical records and may include the following specific information: name, address, driver’s license, financial account information, Social Security number, date of birth, medical history, diagnosis/conditions, lab/test results, treatment information, medications, health insurance information, and/or claims information. There is no indication that any such information was viewed or stolen by an unauthorized actor in relation to this incident. However, Monterey Health Center is unable to prove that such access did not occur.

What We Are Doing. Monterey Health Center takes this incident and the security of patient information in its care very seriously. As part of its ongoing commitment to the privacy and security of patient information, it is working to review existing policies and procedures and to implement additional safeguards to further secure the information in its systems. Monterey Health Center is also notifying the U.S. Department of Health and Human Services, other government regulators, as required, and prominent news media outlets in the state of Oregon.

What Potentially Affected Individuals Can Do. You can find out more about how to protect against potential identity theft and fraud in the below *Steps You Can Take to Prevent Fraud and Identity Theft*. Monterey Health Center encourages you to remain vigilant against incidents of identity theft by reviewing your Explanation of Benefit and account statements regularly and keeping a close eye on your credit card activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order a 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 their credit report.

For More Information. If you have additional questions, please call our dedicated assistance line at 1-888-401-0428, Monday through Friday, during the hours of 8:00 a.m. to 5:00 p.m., Pacific Time. You may also write to the Monterey Health Center at 6975 SE Lake Road, Milwaukie, OR 97267.

STEPS YOU CAN TAKE TO PREVENT FRAUD AND IDENTITY THEFT

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 2000 Chester, PA 19016 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 2002 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.

For Maryland residents: The Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, 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.