Cedar Springs Hospital – Notice of Data Incident
December 9, 2020

Cedar Springs Hospital is providing notice of an incident that may affect the security of some information relating to Cedar Springs Hospital patients. *Cedar Springs Hospital has no evidence of any actual or attempted misuse of any information as a result of this incident*, but is providing this notice in an abundance of caution to provide details of the incident, our response, and resources available to help Cedar Springs patients protect their information from possible misuse, should they feel it appropriate to do so.

Cedar Springs Hospital recently received a request from its licensing agency, the Colorado Department of Public Health & Environment ("CDPHE"), for certain hospital records. As a licensed healthcare provider, Cedar Springs Hospital is subject to periodic surveys by CDPHE and in connection with those surveys, the CDPHE is entitled to various hospital records, including, but not limited to, those containing patient health information. In late October, in connection with a survey, the CDPHE requested Cedar Springs Hospital copy a number of records onto an external drive that CDPHE provided to the facility. Cedar Springs Hospital complied with the request. On October 28, 2020, CDPHE notified Cedar Springs Hospital that the surveyor misplaced the external device containing the documents. Cedar Springs Hospital learned at that time that, contrary to CDPHE's policy, the external device that the CDPHE surveyor provided for use was not encrypted. CDPHE could not rule out the possibility that an unauthorized individual could access the information, if that individual obtained possession of the CDPHE external device. Cedar Springs Hospital immediately began investigating what patient-specific information had been copied onto the external device. On November 9, 2020, Cedar Springs Hospital completed its review and confirmed the records that were downloaded to the external device which were provided to, and misplaced by, CDPHE. The investigation determined that the type of information provided to CDPHE included name, address, date of birth, Social Security Number, medical record number, patient identification number, health insurance information (including health insurance number), treatment history (including dates of treatment, treatment location, and treating physician), medical diagnosis information, and prescription information.

The confidentiality, privacy, and security of patient information is among Cedar Springs Hospital's highest priorities, and Cedar Springs Hospital takes this incident very seriously. Upon learning of this incident, Cedar Springs Hospital moved quickly to investigate and to identify the individuals whose information was potentially impacted. Cedar Springs Hospital has strict policies and procedures in place to protect the information of patients in its care and is evaluating safeguards to prevent a similar event from occurring again. Cedar Springs Hospital is working with CDPHE to obtain additional information about the incident, including why CDPHE policy was not followed and why an unencrypted external device was utilized. Cedar Springs Hospital is notifying individuals whose information may have been impacted by this incident and is providing general information on what they can do to protect their information.

For additional questions, Cedar Springs Hospital has established a dedicated assistance line that may be reached at 800-686-4153 7:00 am to 7:00 pm Mountain Time Monday through Friday (excluding some U.S. national holidays). Individuals can also write to Cedar Springs Hospital Attn: Risk Department at 2135 Southgate Road, Colorado Springs, CO 80906.

Monitor Accounts

In general, we encourage individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious activity. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit reporting 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 your credit report. This notice has not been delayed by law enforcement.

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 consent. However, 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 30348-5788
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. 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 years, 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, 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 one-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-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

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; https://www.consumer.ftc.gov/features/feature-0014-identity-theft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those individuals 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.