Pawnee County Memorial Hospital
One Team - One Mission

Notice Regarding Recent Security Incident

Pawnee County Memorial Hospital (PCMH) in Pawnee City, Nebraska recently experienced a cyber security incident involving some patients' personal health information. On November 29, 2018, PCMH discovered that a malware virus had entered its business e-mail system and may have resulted in unauthorized access to protected health information of some patients. PCMH immediately began an investigation and hired a forensic computer investigator to determine what happened.

The investigation found that a PCMH employee received a malicious e-mail that appeared to be from a trusted source. The e-mail contained what appeared to be a legitimate attachment, and the employee opened the attachment. The malware virus was activated when the employee opened the attachment, and allowed the attackers access to PCMH's e-mail accounts between November 16, 2018 and November 24, 2018. PCMH employees use e-mail as part of the organization's healthcare operations and patient care, and some of the PCMH e-mail accounts included e-mails and/or attachments with internal business reports, clinical reports/summaries, and other documents with protected health information. The attack did not impact the electronic medical record system or patient portal.

According to computer experts and law enforcement, these types of attacks are usually financially motivated and not focused on obtaining patient information. However, because there is a possibility that the information could have been accessed, PCMH is providing notice to all impacted individuals.

The information involved in the incident included full name and one or more of the following: address, date of birth, date(s) of service, medical record number, clinical information (for example, diagnoses and lab results), insurance information, and driver's license/State ID number. For some individuals, the information also included Social Security Number.

After learning about the incident, PCMH took immediate steps to help prevent future intrusions, including a reset of all e-mail account passwords. PCMH continues to work with computer experts to add technology safeguards. PCMH will continue to evaluate its information security practices and implement appropriate steps intended to help secure patients' information.

PCMH has sent letters to all impacted individuals for whom PCMH has valid addresses by U.S. mail. The letters contain important information about steps individuals can take to help prevent medical identity theft or fraud.

PCMH has arranged for a one-year enrollment in an online credit monitoring service (myTrueIdentity) provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. Instructions on how to enroll in this free service are included in the letters sent to affected individuals.

Below is information about other precautionary measures affected individuals can take, including placing a fraud alert and/or security freeze on credit files and obtaining a free credit report

Individuals who have questions or concerns about this incident can call a confidential, toll-free hotline that is staffed with professionals familiar with this incident who can assist with questions and the steps impacted individuals can take to protect against identity theft and fraud. **The**

hotline is available at 1-877-291-9482, Monday through Friday, from 8 am – 8 pm Central Standard Time.

PCMH takes the privacy and security of patients' information very seriously and deeply regrets any inconvenience this attack may have caused patients and their families.

- ADDITIONAL PRIVACY SAFEGUARDS INFORMATION -

Fraud Alert Information

Whether or not you enroll in credit monitoring, we recommend that you place a "Fraud Alert" on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies so you do not need to contact each of them separately. The contact information for the three nationwide credit reporting companies is:

Equifax	TransUnion	Experian
PO Box 740256	PO Box 2000	PO Box 9554
Atlanta, GA 30374	Chester, PA 19016	Allen, TX 75013
www.equifax.com	www.transunion.com/fraud	www.experian.com
1-800-525-6285	1-800-680-7289	1-888-397-3742

Free Credit Report Information

Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the Federal Trade Commission (FTC) at www.identitytheft.gov or at 1-877-ID-THEFT (1-877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations. Also visit the FTC's website at www.ftc.gov/idtheft to review their free identity theft resources such as their comprehensive step-by-step guide "Identity Theft - A Recovery Plan".

Security Freeze Information

You can request a "Security Freeze" on your credit file by sending a request in writing, by mail, to each of the three nationwide credit reporting companies. When a Security Freeze is added to your credit report, all third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. The Security Freeze may delay, interfere with or prohibit the timely approval of any subsequent request or application you make that involves access to your credit report. This may include, but is not limited to, new loans, credit, mortgages, insurance, rental housing, employment, investments, licenses, cellular phone service, utility service, digital signature service, Internet credit card transactions and extension of credit at point of sale. There may be a fee for placing, temporarily lifting, or removing a Security Freeze with each of the nationwide consumer reporting companies, although that fee is waived if you send the credit reporting company proof of eligibility by mailing a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

To place a Security Freeze on your credit files at all three nationwide credit reporting companies, write to the addresses below and include the following information:

Equifax Security Freeze PO Box 105788 Atlanta, GA 30348 https://www.freeze.equifax.com 1-800-685-1111	TransUnion Security Freeze PO Box 2000 Chester, PA 19016 http://transunion.com/freeze 1-888-909-8872	Experian Security Freeze PO Box 9554 Allen, TX 75013 http://experian.com/freeze 1-888-397-3742

- Your full name (first, middle, last including applicable generation, such as JR., SR., II, III, etc.) Your Social Security Number
- Your date of birth (month, day and year)
- Your complete address including proof of current address, such as a current utility bill, bank or insurance statement or telephone bill
- If you have moved in the past 2 years, give your previous addresses where you have lived for the past 2 years
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
- Include applicable fee. Call or visit each of the credit reporting company websites listed above for information on fees for Security Freeze services. Forms of payment are check, money order, or credit card (American Express, Discover, MasterCard and Visa), or a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

Within 5 business days of receiving your request for a security freeze, the consumer credit reporting company will provide you with a personal identification number (PIN) or password to use if you choose to remove the freeze on your consumer credit report or to authorize the release of your consumer credit report to a specific party or for a specified period of time after the freeze is in place.