Sauk Prairie Healthcare ("Sauk Prairie"), a nonprofit 501(c)(3) acute care hospital provider, is providing notice to current and former patients of a ransomware attack involving our third-party bad debt account vendor, Personal Finance, Company, Inc. ("PFC") which may have led to the potential exposure of certain personal information.

What Happened? On or about May 5, 2022, Sauk Prairie was notified by our third-party bad debt account vendor, Personal Finance Company, Inc. ("PFC") of a security breach. On, February 26, 2022, PFC detected a ransomware attack in which an unauthorized third party accessed and disabled some of PFC's computer systems. PFC reports that they immediately engaged third-party forensic specialists to assist them with securing their network environment and investigating the extent of any unauthorized activity. Federal law enforcement was also notified. The investigation determined an unauthorized third party may have accessed files containing certain individuals' personal information.

What Information Was Involved? As a result of this incident, PFC determined that the following information could have been accessed by an unauthorized third party: first and last name, address, accounts receivable balance and information regarding payments made to accounts, and, in some cases, date of birth, Social Security number, and health insurance and medical treatment information.

What Are We Doing? We take the security of sensitive information very seriously. We are working closely with PFC to ascertain the scope of this incident. We remain committed to fostering a culture of privacy in our organization.

Notification. While the investigation found no evidence that individual information has been specifically misused to date, PFC is mailing letters to potentially impacted individuals with details about the incident and providing resources they can use to help protect their information. PFC is also offering potentially impacted individuals access to free credit monitoring and identity theft protection services through Cyberscout, a leading identity protection company.

Patients receiving a notice from PFC should consider taking the steps outlined to protect themselves.

We, at Sauk Prairie, take the security of our patients' data very seriously. Although this ransomware attack did not involve our systems, we are issuing this website notification in an abundance of caution to all current and former patients of Sauk Prairie.

Fraud Prevention We encourage the potentially affected individuals to remain vigilant against incidents of identity theft and fraud and to seek to protect against possible identity theft or other financial loss by regularly reviewing their financial account statements, credit reports, and explanations of benefits for suspicious activity.

PFC is providing a dedicated toll-free call center for potentially affected individuals who have questions, want to enroll in credit monitoring and identity theft protection services, or who want to learn additional steps to protect their information. To contact the call center, please call 1-844-663-3160, between 6am and 6pm MST.

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

ADDITIONAL RESOURCES

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. For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. 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. 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. 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	TransUnion Security Freeze	Experian Security Freeze
PO Box 105788	PO Box 160	PO Box 9554
Atlanta, GA 30348	Woodlyn, PA 19094	Allen, TX 75013
http://www.freeze.equifax.com	http://transunion.com/freeze	http://experian.com/freeze
1-800-349-9960	1-888-909-8872	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.

Additional Information for residents of the following states:

California: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

Kentucky: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

Massachusetts: Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information

from your state attorney general at: *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

New Mexico: 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 a 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. You can 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.

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Oregon: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

West Virginia: You have the right to ask that nationwide consumer reporting agencies place fraud alerts in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.