Bigfork Valley Hospital Notifies Individuals of Data Security Incident

Bigfork MN – March 25, 2025 – Bigfork Valley Hospital ("Bigfork Valley") has learned of a data security incident that may have involved the personal and/or protected health information belonging to individuals. Bigfork Valley has sent notice to this incident to potentially affected individuals and provided resources to assist them.

On or about January 28, 2025, Bigfork Valley learned that personal information of certain individuals was potentially accessed without authorization. The unauthorized access was the result of a suspicious event first learned of on or about November 26, 2024. Specifically, Bigfork Valley identified suspicious activity associated with one (1) email account. Upon learning of this activity, Bigfork Valley immediately took steps to secure its email environment and engaged digital forensics specialists to assist with the investigation.

The investigation determined that certain emails and attachments were accessed or acquired without authorization on November 4, 2024. Following this confirmation, Bigfork Valley conducted a comprehensive review of the potentially affected data and determined that personal information belonging to certain individuals, may have been accessed in connection with this incident. Bigfork Valley then worked diligently to effectuate notification to potentially affected individuals. Please note, Bigfork Valley has no evidence of the misuse or attempted misuse of any potentially accessed information. However, on March 25, 2025, Bigfork Valley sent notification letters to the individuals potentially involved in this incident providing them information about what happened and steps they can take to protect their personal information. We take the security of personal and/or protected health information very seriously and are taking steps to prevent a similar event from occurring in the future, including implementing new technical safeguards and security as well as periodic technical and nontechnical evaluations.

Based on the investigation of the incident, the following personal and protected health information may have been affected as a result of the incident: name, phone number; date of birth; social security number; financial account number, driver's license or state identification number, patient account number, Medicare or Medicaid number, health insurance member number; cost of treatment, diagnosis, treatment, or procedure information, medical history or allergies, prescription drug information, lab test results or images, date of admission or treatment, treatment location, and healthcare provider name.

We established a toll-free call center to answer questions about the incident and address related concerns. The call center is available Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time and can be reached at 1-833-998-7840.

The privacy and protection of personal and protected health information is a top priority for Bigfork Valley. We deeply regret any inconvenience or concern this incident may cause.

While we have no evidence of the misuse, or attempted misuse of any potentially affected individual's information, we are providing the following information to help those wanting to know more about steps they can take to protect themselves and their personal information:

What steps can I take to protect my personal information?

- Please notify your financial institution immediately if you detect any suspicious activity on any of your accounts, including unauthorized transactions or new accounts opened in our name that you do not recognize. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities.
- You can request a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To do so, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is listed at the bottom of this page.
- You can take steps recommended by the Federal Trade Commission to protect yourself from identify theft. The FTC's website offers helpful information at www.ftc.gov/idtheft.
- Additional information on what you can do to better protect yourself is included in your notification letter.

How do I obtain a copy of my credit report?

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Use the following contact information for the three nationwide credit reporting agencies:

TransUnion	**Experian**	**Equifax**
P.O. Box 2000	P.O. Box 9532	P.O. Box 105851
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348
1-800-916-8800	1-888-397-3742	1-800-525-6285
www.transunion.com	www.experian.com	www.equifax.com

How do I put a fraud alert on my account?

You may consider placing a fraud alert on your credit report. This fraud alert statement informs creditors to possible fraudulent activity within your report and requests that your creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact Equifax, Experian or TransUnion and follow the Fraud Victims instructions. To place a fraud alert on your credit accounts, contact your financial institution or credit provider. Contact information for the three nationwide credit reporting agencies is included in the letter and is also listed at the bottom of this page.

How do I put a security freeze on my credit reports?

You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or online by following the instructions found at the websites listed below. You will need to provide the following information when requesting a security freeze (note that if you are making a request for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) address. You may also be asked to provide other personal information such as your email address, a copy of a government-issued identification card, and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. There is no charge to place, lift, or remove a freeze. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	Experian Security Freeze	TransUnion (FVAD)
PO Box 105788	PO Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-909-8872
www.equifax.com	www.experian.com	www.transunion.com

What should I do if my family member was involved in the incident and is deceased?

You may choose to notify the three major credit bureaus, Equifax, Experian and Trans Union, and request they flag the deceased credit file. This will prevent the credit file information from being used to open credit. To make this request, mail a copy of your family member's death certificate to each company at the addresses below.

Equifax	**Experian**	**TransUnion**
Equifax Information Services	Experian Information Services	Trans Union Information
P.O. Box 105169,	P.O. Box 9701	Services
Atlanta, GA 30348	Allen, TX 75013	P.O. Box 2000
		Chester, PA 19022