On Sapphire Letterhead

[Date]

Name
Address
City, Sate Zip Code

Dear Valued Patient:

Sapphire Community Health (Sapphire) is committed to patient privacy. We take patient privacy very seriously and it is important to us that you are made fully aware of a potential privacy issue.

What happened: On February 18, 2021, Sapphire was the victim of a ransomware attack. An unknown party was able to access some of Sapphire's data files and use an encryption code to "lock" those files and make them unusable. No patient medical records were affected and Sapphire's investigation of the attack did not indicate that any personal information was acquired or used by an unauthorized individual. However, because the encrypted files contained personal information, we are notifying all of our patients of the attack so that you can take appropriate steps to protect yourself from possible harm.

Sapphire's response: Sapphire has taken several steps to mitigate any further harm to our anyone whose information was affected. Immediately after discovery, Sapphire shut down its information systems to prevent the attack from spreading further and took appropriate scanning and restoration steps. Sapphire reported the attack to law enforcement and immediately began conducting a forensic security investigation. Sapphire continues to evaluate and implement additional security safeguards to protect against future attacks.

Information affected: The personal information contained in the encrypted files that may have been compromised included names, addresses, dates of birth, and for a limited number of individuals, social security numbers and bank account numbers.

Steps you should take to protect yourself: Sapphire's investigation of the attack did not indicate that any personal information was acquired or used by an unauthorized individual. However, because we cannot conclusively determine that the information was not compromised, we are sending you this letter so that you can take appropriate steps to protect yourself from any harm that could arise from the attack. You may want to take one or more of the following actions:

- *Fraud Alert*. Call the toll-free numbers of any one of the three major credit bureaus (below) to place a fraud alert on your credit report. 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. This can help prevent an identity thief from opening additional accounts in your name.

    - **Equifax:** 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241.
    - **Experian:** 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013.
    - **TransUnion:** 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

- *Order credit reports*. You can order a free copy of your credit report from the three credit reporting companies listed above using the website or telephone number below:
    www.annualcreditreport.com

1-877-322-8228

When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that you did not open.

- *Monitor credit reports*. Continue to monitor your credit reports. Even if you place a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information.

Contact information: If you have questions or want to learn additional information about the incident, you may contact us at **406-802-2880**.

We sincerely apologize for any inconvenience this situation may cause you. Sapphire is committed to providing quality health care services to our community and we take our obligation to protect your personal information seriously. If you have any questions, please do not hesitate to use the contact information provided above.

Sincerely,

All of us at Sapphire Health

On Sapphire Letterhead

[Date]

Name
Address
City, Sate Zip Code

To our Valued Employees (Current and Past):

As you know, Sapphire is committed to protecting the privacy and security of our patients' and employees' personal information. We are writing to let you know about a recent cybersecurity incident that may have affected your personal information contained in Sapphire's employment files.

What happened: On February 18, 2021, Sapphire was the victim of a ransomware attack. An unknown party was able to access some of Sapphire's data files and use an encryption code to "lock" those files and make them unusable. No patient medical records were affected and Sapphire's investigation of the attack did not indicate that any personal information was acquired or used by an unauthorized individual. However, because the encrypted files contained personal information, including information contained in employment files, we are notifying all you of the attack so that you can take appropriate steps to protect yourself from possible harm.

Sapphire's response: Sapphire has taken several steps to mitigate any further harm to our anyone whose information was affected. Immediately after discovery, Sapphire shut down its information systems to prevent the attack from spreading further and took appropriate scanning and restoration steps. Sapphire reported the attack to law enforcement and immediately began conducting a forensic security investigation. Sapphire continues to evaluate and implement additional security safeguards to protect against future attacks. Additionally, Sapphire has arranged for LifeLock identity threat protection to be made available to you at no cost. Please contact us at **406-802-2880** if you would like more information about this.

Information affected: The personal information contained in the encrypted files that may have been compromised included names, addresses, dates of birth, and for a limited number of individuals, social security numbers and bank account numbers.

Steps you should take to protect yourself: Sapphire's investigation of the attack did not indicate that any personal information was acquired or used by an unauthorized individual. However, because we cannot conclusively determine that the information was not compromised, we are sending you this letter so that you can take appropriate steps to protect yourself from any harm that could arise from the attack. You may want to take one or more of the following actions:

- *Fraud Alert*. Call the toll-free numbers of any one of the three major credit bureaus (below) to place a fraud alert on your credit report. 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. This can help prevent an identity thief from opening additional accounts in your name.

    - **Equifax:** 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241.
    - **Experian:** 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013.
    - **TransUnion:** 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

- *Order credit reports*. You can order a free copy of your credit report from the three credit reporting companies listed above using the website or telephone number below:

  www.annualcreditreport.com
  1-877-322-8228

  When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that you did not open.

- *Monitor credit reports*. Continue to monitor your credit reports. Even if you place a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information.

Contact information: If you have questions or want to learn additional information about the incident, you may contact us at **406-802-2880**.

We sincerely apologize for any inconvenience this situation may cause you. Sapphire is committed to providing quality health care services to our community and we take our obligation to protect your personal information seriously. If you have any questions, please do not hesitate to use the contact information provided above.

Sincerely,

All of us at Sapphire Health