Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Re: <<Variable Data 1>>

Dear <<Full Name>>,

Family Christian Health Center ("FCHC") is writing to notify you of a recent data incident that impacted the security of certain information stored on our company's network. This letter provides an overview of the event and steps we are taking in response.

What Happened?
On February 26, 2025, Family Christian Health Center became aware of a security incident occurring on our network. Based on our investigation to date, we determined that an unauthorized actor gained access to certain systems between February 23 – 25 2025. After completing a detailed review of the compromised systems, we discovered on April 1, 2025, that the data potentially included information related to patients and employees. We then conducted a comprehensive analysis of the affected files and confirmed that the incident involved both personal information and protected health information.

What information was involved?
The information present in the files that may have been viewed or acquired as a result of this incident included your name and <<Breached Elements>>.

What are we doing?
FCHC values the privacy and security of our patients' information. Upon learning of the incident, we immediately launched an investigation with the assistance of a leading outside forensic security firm to determine the nature and scope of the activity and confirm the security of our computer systems and network. We also reported the incident to law enforcement. Since the incident we have implemented a series of cybersecurity enhancements, including installation of additional endpoint detection and response software, resetting all passwords, and rebuilding affected servers. We will continue to assess our policies and procedures already in place for ways to defend against evolving threats.

What can you do?
As with any data incident, we encourage you to remain vigilant for incidents of fraud or misuse from any source and consider taking steps to avoid identity theft, obtain additional information, and protect your personal information. If you find any errors or unauthorized activity, you should contact your financial institution or the appropriate service provider. You may also file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. More steps are described below.

For more information
For additional questions, please feel free to contact the toll-free call center at (855)-260-8164, Monday through Friday, between 9:00 a.m. and 9:00 p.m. Eastern Time except holidays. You will need to reference the FCHC Incident when calling.

We sincerely apologize for this situation and any inconvenience it may cause you.

Sincerely,

Dr. Lisa Green
Chief Executive Officer
Family Christian Health Center

ADDITIONAL STEPS TO HELP PROTECT YOUR INFORMATION

Avoiding Medical ID Theft. The following practices can provide additional safeguards to protect against medical identity theft.

- Regularly check the accounts you use regularly to pay for health-related expenses, including bank accounts, health savings accounts, credit card accounts.
- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

Review Personal Account Statements and Credit Reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax	Experian	TransUnion
1-888-298-0045	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

Report Suspected Fraud. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. When you place a fraud alert, it will last one year. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years. To place a fraud alert, contact the nationwide credit reporting agencies by phone or online. For more information, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

Obtain additional information about the steps you can take to avoid identity theft from the following entities:

- ***District of Columbia residents***: District of Columbia Attorney General, 400 6th Street, NW, Washington, DC 20001; https://oag.dc.gov; 202-727-3400.
- ***Maryland residents***: Maryland Attorney General, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; https://www.marylandattorneygeneral.gov or 1-410-528-8662 or 1-888-743-0023.
- ***New Mexico residents***: 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 information 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 bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting bureaus may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to your 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 violators. You may have additional rights under the Fair Credit Reporting Act not summarized here**.** Identity theft victims and active-duty military personnel have additional specific rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf; and by contacting Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave NW, Washington, DC 20580.
- ***New York residents***: Office of the New York Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov; or 1-800-771-7755.
- ***North Carolina residents***: North Carolina Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; https://ncdoj.gov; and toll-free at (877) 566-7226 or (919) 716-6000.
- ***All U.S. Residents***: The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and/or the Federal Trade Commission ("FTC"). You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC at 1-877-IDTHEFT (1-877-438-4338) or https://consumer.ftc.gov/features/identity-theft. The mailing address for the FTC is:

  Federal Trade Commission, Consumer Response Center
  600 Pennsylvania Avenue, NW
  Washington, DC 20580