Notice to Individuals Regarding Privacy Incident

First Street Family Health ("FSFH") is providing notice to individuals about a privacy incident it discovered on July 16, 2022. Parts of FSFH's computer network were subject to a cyber-attack impacting some files containing patients' protected health information. The cyber-attack resulted in the automated deletion of electronic files containing protected health information. In addition, for the small percentage of patients who had medical referral forms on file, there may have been unauthorized viewing and acquisition of those referral forms. FSFH was able to fully restore many files from the backups that were untouched by the attack. However, electronic medical records from June 28, 2021, to July 15, 2022, have not been recovered because those backups were deleted in the incident. There is no indication the deleted files were first viewed or exported by the cyber criminal. FSFH was not locked out of the files through encryption as is often the case. Instead, its files were programmatically deleted. FSFH's experts determined the unauthorized access began as early as July 5, 2022 and ended after discovery on July 16. FSFH mailed notice letters on August 26, 2022 to involved patients at their last known mailing addresses.

FSFH promptly investigated and worked to restore and continuously monitor its systems and block further access. FSFH performed a full password reset and enhanced protective measures that were in place before this incident. FSFH engaged a national cybersecurity firm to assist in analyzing the nature and scope of what happened and to review security practices and help strengthen security protocols going forward. FSFH has reported the crime to federal law enforcement for further investigation.

The type of information involved may have included full name, address, date of birth, phone number, email address, social security number, dates of service, nature of services including diagnoses, conditions, lab results, medications, health insurance identification cards and numbers, and billing information. It did not include financial account or payment card information.

FSFH wants to make potentially impacted individuals aware of steps they may take to guard against potential harm. FSFH encourages individuals to remain vigilant to the possibility of fraud and identity theft by regularly reviewing their financial statements, credit reports, and explanation of benefits (EOBs) from their health insurers for any unauthorized activity. If individuals identify services they did not receive or accounts, charges, or withdrawals that they did not authorize, they should report to the involved company or credit-reporting agency immediately and to local law enforcement. Individuals can obtain information about placing fraud alerts and security freezes from the Federal Trade Commission and the three national credit reporting agencies at the toll-free numbers, websites, or mailing addresses as follows:

Federal Trade Commission	Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-877-382-4357	1-866-349-5191	1-888-397-3742	1-800-680-7289
600 Pennsylvania Ave., NW	P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

FSFH has arranged for adult individuals with information involved in this incident to be eligible to enroll, at no charge, in 12 months of Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services, and for parents of involved minors to be eligible to enroll, at no charge, in 12 months of Cyber Monitoring services, and proactive fraud assistance service. The services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. To take advantage of this service, an individual will need to first obtain and use their unique enrollment code which can be found in the notice letter mailed on August 26, 2022. For individuals who did not receive a notice letter but whose information may have been involved, they must contact the toll-free number below to determine if their information was involved and, if so, to receive a free enrollment code. Please note the deadline to enroll in the free monitoring services is **November 23, 2022**.

FSFH has partnered with CyberScout to set up a call center for 90 days to answer questions about this incident or about enrollment in the monitoring service. Individuals who have questions, including whether their personal information was involved, should call the toll-free help line **1-800-405-6108** between 6:00 am to 6:00 pm Mountain time, Monday through Friday (closed on holidays). The call center can provide additional information and answers to many questions for individuals whose information was potentially involved in this incident.

Recommended Steps to Help Protect Your Information

1. Telephone. Contact the toll-free help line **1-800-405-6108** to gain additional information about this event.

2. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, even if you do not enroll through Identity Force, you 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 1-877-322-8228. 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 and have enrolled through Identity Force, notify them immediately by calling and requesting help. You should also know that you have the right to file a police/sheriff's report if you ever experience identity fraud. Please note that to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General in your State.

3. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only one of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

4. Security Freeze. 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. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

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

Colorado Residents: Visit the Stop Fraud Colorado website created by the Colorado Attorney General at https://www.stopfraudcolorado.gov/fraud-center/identity-theft.html.

Kentucky Residents: 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 Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 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 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/201904_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 Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

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

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

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.