

Notice of Data Event

Fertility Centers of Illinois (“FCI”) is providing notice of a recent incident that may affect the security of certain information relating to some FCI patients.

On February 1, 2021, FCI became aware of suspicious activity on its internal systems. In response, FCI engaged independent forensic investigators to conduct an investigation of the activity. The investigation revealed that an unauthorized third party had gained access to a number of FCI’s administrative files, and folders containing certain data. Due to the security systems already in place, the investigation indicated that **no EMR (electronic medical records) systems were accessed or otherwise compromised as a result of this incident.** FCI took immediate steps to conduct a thorough and comprehensive review of its records to identify the files accessed, the information contained in those files, and to whom that information pertained. On August 27, 2021, FCI determined that information related to certain FCI patients was included in the set of files accessed by the unauthorized third party. FCI is not aware of any actual or attempted misuse of patient information as a result of this incident.

The impacted files contained personal information including the names of some patients, employer-assigned identification numbers, passport numbers, Social Security numbers, financial account information, payment card information, treatment information, diagnosis, treating/referring physicians, medical record number, medical billing/claims information, prescription/medication information, Medicare/Medicaid identification information, health insurance group numbers, health insurance subscriber numbers, patient account numbers, encounter numbers, ill health / retirement information, master patient index, occupational-health related information, other medical benefits and entitlements information, other medical identification numbers, patkeys/reason for absence, sickness certificate, usernames and passwords with PINs or account login information, and medical facilities associated with patient information.

What We Are Doing. Safeguarding the privacy of your information and the security of our network is among our highest priorities. We have strict security measures in place to protect information in our care. Upon learning of this incident, FCI immediately took steps to eliminate unauthorized access and brought in independent forensic investigators to investigate and remediate the matter. Additional security measures have been taken since the incident to further secure access to data, individual accounts, and equipment, including the implementation of enterprise identity verification software. Additionally, all FCI employees have received enhanced training on security practices. Please be assured that we have invested considerable resources to ensure that such a vulnerability does not exist in the future.

As an added precaution, we are offering affected parties access to credit monitoring and identity theft protection services for 12 months through Equifax at no cost.

We encourage impacted parties to remain vigilant against incidents of identity theft and fraud by reviewing account statements and explanation of benefits forms, and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. We also encourage you to review the below Steps You Can Take to Protect Personal Information.

We understand that you may have questions about this incident that are not addressed in this letter. If so, please contact our toll-free dedicated assistance line at 855-604-1736 9:00 am to 9:00 pm Eastern Monday through Friday (excluding some U.S. national holidays). You may also write to FCI at 2555 Patriot Avenue Glenview, IL 60026.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade

Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For 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 bureaus 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 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. We encourage you to 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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. No Rhode Island residents are identified to be impacted by this incident.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.