Notice of a Data Breach

Extend Fertility is notifying individuals whose information was involved in a recent data security incident.

On December 20, 2021, we discovered a ransomware incident that impacted our networks and servers which contained protected health and personal information of some of our patients. After discovering the incident, we quickly took steps to secure and safely restore our systems and operations. We engaged outside counsel and third-party forensic experts to assist in the remediation efforts and conduct a thorough investigation of the incident's nature and scope. We also contacted the FBI to seek assistance and guidance, as one of the many health care providers confronting the impacts of the evolving cyber threat landscape.

We concluded our initial investigation on January 28, 2022. The investigation determined that on or about December 15, 2021, an unauthorized individual accessed our systems and likely obtained some information. We have undertaken an extensive analysis of our files to determine what information was involved and to identify individuals whose data was potentially impacted. Although the data analysis is ongoing, in the interest of initiating notifications, we are in the process of informing those individuals whose personal information may have been accessed or obtained.

The types of information potentially involved include demographic information (i.e., first and last name, gender, home address, phone number, email address, and date of birth); clinical information (i.e., medical history/diagnosis/treatment, dates of service, lab test results, prescription information, provider name, medical account number, or anything similar in your medical file and/ or record); and financial information (i.e., health insurance policy and group plan number, group plan provider, and claim information).

As of now, we have no evidence indicating that any information has been used for identity theft or financial fraud. However, out of an abundance of caution, we are notifying individuals of the incident and providing information on steps individuals can take to help protect their information.

We are offering complimentary credit monitoring and identity protection services to individuals impacted or involved in the incident. If interested in signing up for the complimentary credit monitoring, individuals must do so within 90 days of receiving their notification letter from us. If you believe you were impacted by this incident and wish to take advantage of these services, please contact the dedicated toll-free helpline (as stated below) and for more information about tips to protect from identity theft, please see the “other important information.”

We take the responsibility to protect the security and privacy of the information in our care with the utmost seriousness, and we sincerely regret the concern and inconvenience caused by this event. In response to this incident, we are implementing additional safeguards to our existing cybersecurity infrastructure and enhancing its employee cybersecurity training. Further, we are working with its external cybersecurity experts to improve our cybersecurity policies, procedures, and protocols to help minimize the likelihood of this type of incident occurring again.

For individuals seeking more information or who have questions, we established a dedicated toll-free helpline set up specifically for this purpose at 1-800-364-0049 from 8:00 am to 8:00 pm Eastern time, Monday through Friday (except holidays). Representatives are available for 90 days. In addition, individuals seeking to contact us directly may write to 200 West 57th Street #1101, New York, NY 10019.

OTHER IMPORTANT INFORMATION

Obtain and Monitor Your Credit Report. We recommend that you obtain a free copy of your credit report from each of the three nationwide credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at: https://www.annualcreditreport.com/index.action.

Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below to request a copy of your credit report or general identified above inquiries.

Equifax	**Experian**	**TransUnion**
(888) 766-0008	**(888) 397-3742**	**(800) 680-7289**
P.O. Box 740256	P.O. Box 2104	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze (also known as a Credit Freeze). Following is general information about how to request a security freeze from the three credit reporting agencies. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. In addition, in some states, the agency cannot charge you to place, lift or remove a security freeze. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided above).

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/	**Experian Security Freeze** P.O. Box 9554 Allen, TX 75013 www.experian.com/freeze	**TransUnion** **Security Freeze & Fraud Victim Assistance Dept.** P.O. Box 160 Woodlyn, PA 19094 https://www.transunion.com/credit-freeze

Consider Placing a Fraud Alert on Your Credit Report. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three nationwide credit reporting agencies identified above. Additional information is available at https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Remain Vigilant, Review Your Account Statements and Notify Law Enforcement of Suspicious Activity. As a precautionary measure, we recommend that you remain vigilant by closely reviewing your account statements and credit reports. If you detect any suspicious activity on an account, we strongly advise that you promptly notify the financial institution or company that maintains the account. Further, you should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint or to contact the FTC, you can (1) send a letter to the *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; (2) go to IdentityTheft.gov/databreach; or (3) call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

Take Advantage of Additional Free Resources on Identity Theft. We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). In addition, a copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/.

District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 200001, 202-727-3400, www.oag.dc.gov. **Iowa residents** may also wish to contact the Office of the Attorney general on how to avoid identity theft by calling 515-281-5164 or by mailing a letter to the Attorney General at: *Office of the Attorney General of Iowa,* Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.**Maryland residents** may wish to review the information the Attorney General, who can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, or visiting www.oag.state.md.us. **Massachusetts residents**: State law advises you that you have the right to obtain a police report. You also will not be charged for seeking a security freeze, as described above in this document. **New Hampshire residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the

security freeze, please contact three credit reporting agencies identified above. **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. **New York Residents**: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: *New York Attorney General's Office Bureau of Internet and Technology*, (212) 416-8433, https://ag.ny.gov/internet/resource-center and or NYS Department of State's Division of Consumer Protection, (800) 697-1220, https://www.dos.ny.gov/consumerprotection. **North Carolina residents** may wish to review the information provided by the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/identity-theft/, or by contacting the Attorney General by calling *1-877-566-7226* or emailing or by mailing a letter to the Attorney General at *North Carolina Attorney General's Office* 9001 Mail Service Center Raleigh, NC 27699. **Oregon Residents**: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877- 9392, www.doj.state.or.us. **Rhode Island residents** have the right to obtain a police report (if one was filed. Alternatively, you can file a police report). Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services. **West Virginia residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above.