ProPharma Group provides support services for multiple pharmaceutical companies, including Xeris Pharmaceuticals. As part of these services, ProPharma processes reports of adverse events associated with different medications and treatments. A recent data security incident exposed the personal information of a small number of Xeris customers to an unauthorized third party; for some of these individuals, neither Xeris nor ProPharma has contact information. ProPharma takes the security of personal information very seriously, and sincerely regrets that this occurred. This notice contains more information about the incident. If you are concerned you may be affected, you can inquire with ProPharma using the contact information below.

What Happened?
On April 21, 2024, a small number of ProPharma servers were impacted by a data security incident. With the assistance of external cybersecurity experts, ProPharma immediately investigated to determine the scope of the incident. After an extensive review of the files removed as a result of the incident, ProPharma became aware on July 31, 2024, that some individuals' personal information was included among documents affected by the incident.

What Information Was Involved?
This information included names along with the following: contact information and medical information concerning an adverse pharmaceutical event(s) reported to ProPharma. ProPharma has obtained assurance that the unauthorized third party no longer possesses ProPharma information and has no evidence it has been misused.

What is ProPharma Doing?
ProPharma takes the security of all information in its systems very seriously and has already taken steps to prevent a reoccurrence by increasing monitoring of the impacted networks, further improving access controls, and hardening its systems.

What Can You Do?
ProPharma recommends that you review the additional information below, which contains important steps you can take to protect your personal information.

For More Information
If you would like to request any additional information about this incident, please contact ProPharma at client.enquiries@propharma.com. Protecting your information is important to ProPharma.

Additional Information

Monitoring: You should always remain vigilant for incidents of fraud and identity theft, especially during the next 12-24 months, by reviewing account statements and monitoring your credit reports for suspicious or unusual activity and immediately report any suspicious activity or incidents of identity theft. You have the right to obtain or file a police report. You can contact the Federal Trade Commission (FTC) for more information on preventing identity theft. We encourage you to report any incidents of identity theft to the FTC.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.identitytheft.gov

Credit Reports: You may obtain a copy of your credit report, for free, whether or not you suspect any unauthorized activity on your account, from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You have the right to place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). 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. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. To place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be needed to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-866-478-0027

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
http://www.experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
1-800-916-8800

For residents of *Iowa* and *Oregon*: You are advised to report any suspected identity theft to law enforcement or to the state Attorney General and Federal Trade Commission.

For residents of *New Mexico:* You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:
You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the FTC about fraud alerts, security freezes, and steps you can take to prevent identity theft.

District of Columbia Attorney General
400 6th Street NW
Washington, DC 20001
1-202-442-9828
www.oag.dc.gov

Maryland Office of Attorney General
200 St. Paul Pl
Baltimore, MD 21202
1-888-743-0023
https://www.marylandattorneygeneral.gov/

New York Attorney General
120 Broadway, 3rd Fl
New York, NY 10271
1-800-771-7755
www.ag.ny.gov

North Carolina Attorney General
9001 Mail Service Ctr
Raleigh, NC 27699
1-877-566-7226
https://ncdoj.gov/

Rhode Island Attorney General
150 South Main St
Providence RI 02903
1-401-274-4400
www.riag.ri.gov