Notice of Data Breach

Dear {{User.UserAttributes.FirstName}} {{User.UserAttributes.LastName}},

Acadia Pharmaceuticals Inc. (“Acadia”) experienced a data incident that may have involved some of the personal information that Acadia holds about you. In this case it was the name you used to register on our site only. Acadia takes the protection and proper use of your information very seriously; therefore, we are contacting you to explain the incident and measures taken to protect your information.

What happened?

On October 24 and October 30, 2024, Acadia sent an email to members of our More to Parkinson’s community to welcome them to the community. Acadia subsequently re-sent the same email to the same members of our More to Parkinson’s community on October 29 and November 4, 2024. Due to an internal error, the name of the recipient in the “Dear” line of each email did not match the email address to which the email was sent. As a result, an email regarding the More to Parkinson’s community addressed to you may have been sent to the email address of another individual who is a member of the More to Parkinson’s community. Acadia became aware of this incident on November 4, 2024 and promptly began to investigate and assess the impact of the incident.

What information was involved?

The potentially identifiable information that may have been accessed is the name you used to register for our More to Parkinson’s community. Being a member of the More to Parkinson’s community does not require or indicate a Parkinson’s disease diagnosis, but the context of the email could suggest that you may be an individual that may be interested in Parkinson’s disease. No medical records were disclosed or accessed as a result of this incident. No other identifiable information was disclosed or accessed as a result of this incident, and your registered name was only disclosed to **one other email recipient**.

What we are doing.

At Acadia, the confidentiality, privacy, and security of your information is a top priority, and we take this incident very seriously. Upon first becoming aware of the incident, Acadia immediately commenced an investigation to assess the impact of the incident and to understand how the incident occurred.

As part of our ongoing commitment to the security of your information, we are evaluating our policies and additional measures and quality control checks we can

implement to ensure this type of incident does not happen in the future. We are also providing notification of this incident to applicable U.S. state regulators, including state Attorneys General, where legally required.

What you can do.

Although only your name and potential interest in Parkinson's disease, without any additional information, was disclosed, we still encourage you to be vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring free credit reports for suspicious activity and to detect errors on an ongoing basis. Suspicious activity should be promptly reported to relevant parties, including an insurance company and/or financial institution.

Additional resources can be found below in the attached Steps You Can Take to Help Protect Your Personal Information.

For more information.

We regret this incident occurred and any inconvenience or concern it has caused you. If you have questions, please call (866) 676-7103, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Acadia Pharmaceuticals Inc.

Steps You Can Take to Help Protect Your Personal Information Monitor Your Accounts

If you are a U.S. individual, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 at no cost, 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze

on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

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

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

Equifax

https://www.equifax.com/personal/credit-report-services/

1-888-298-0045

Equifax Fraud Alert

P.O. Box 105069

Atlanta, GA 30348-5069

Equifax Credit Freeze

P.O. Box 105788

Atlanta, GA 30348-5788

Experian

https://www.experian.com/help/

1-888-397-3742

Experian Fraud Alert

P.O. Box 9554

Allen, TX 75013

Experian Credit Freeze

P.O. Box 9554

Allen, TX 75013

TransUnion

https://www.transunion.com/customersupport/contact-us-consumers

1-800-916-8800

TransUnion Fraud Alert

P.O. Box 2000

Chester, PA 19016

TransUnion Credit Freeze

P.O. Box 160

Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer credit reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 727-3400; and https://oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

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 (401) 274-4400. Under Rhode Island law, individuals have the right to file or obtain any police report filed in regard to this event. The number of Rhode Island residents that may be impacted by this event is currently unknown.

For Vermont residents, please note that you should not provide personal information in response to electronic communications regarding security breaches.
