NOTICE OF DATA PRIVACY EVENT

WellDyneRx, LLC ("WellDyne") is providing notice of an incident that could affect the privacy of information of certain individuals for whom it provided pharmacy benefit related services. While we are unaware of any actual or attempted misuse of individually-identifiable information, we take this incident very seriously and are providing information about the incident, our response to it, and resources available to individuals to help protect their information, should they feel it appropriate to do so.

What Happened? On December 2, 2021, WellDyne became aware of suspicious activity related to a WellDyne email account. In response, we began an investigation of the activity with the assistance of third-party forensic investigators to determine the nature and scope of the incident. We determined that there was unauthorized access to the account between October 30, 2021, and November 11, 2021. Although there is no evidence that individually-identifiable information contained within the email account was accessed or taken by an unauthorized party, we cannot rule out this possibility. In response, WellDyne undertook a comprehensive and time-consuming programmatic and manual review of the contents of the email account to determine the type of information stored therein, and to whom the information pertained. On March 11, 2022, we completed this extensive review process, and identified the scope of the information at risk and the population who may be affected. We have worked diligently since this time to confirm the contact information for the individuals who may be impacted and the types of information at issue for each individual, in order to provide an accurate notification.

What Information Was Involved? We conducted a thorough review of the affected email account to identify the types of information stored therein and to whom it related. Although there is no evidence that individually-identifiable information contained within the email account was accessed or taken by an unauthorized party, we cannot rule out this possibility. While the specific types of information varies for each individual, the scope of information involved includes: name, date of birth, Social Security number, driver's license number, treatment information, health insurance information, contact information, prescription information, and other medical/health information.

How Will Individuals Know If They Are Affected By This Incident? We are mailing notice letters to the individuals who were identified as potentially impacted. If an individual does not receive a letter but would like to know if they are affected, they may call our dedicated assistance line, detailed below.

What WellDyne is Doing. The confidentiality, privacy, and security of personal information within our care is among our highest priorities. Upon learning of the event, we secured the compromised account and investigated to identify any individuals that were affected. We have taken additional steps to improve security and better protect against similar incidents in the future. We are also notifying applicable regulators, including the Department of Health and Human Services.

Whom Should Individuals Contact For More Information? If individuals have questions or would like additional information, they may call WellDyne's dedicated assistance line at (877) 389-2455 between the hours of 9am-9pm Eastern Standard Time, Monday through Friday.

What You Can Do. We encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits forms, and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report, place a fraud alert, or a security freeze. Contact information for the credit bureaus is below:

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, 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 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.