NOTICE OF DATA PRIVACY INCIDENT

Pivot Health writes to inform you of a recent event that may affect the confidentiality of some of your information. Although we are unaware of any identity theft or fraud occurring as a result of this event, we are providing you with information about the event, our response, and resources available to help you protect your information, should you feel it appropriate to do so.

What Happened? On or around March 13, 2026, Pivot Health became aware of suspicious activity within our Amazon Web Services ("AWS") environment. We immediately took steps to secure our systems and launched an investigation into the nature and scope of the activity with the assistance of third-party forensic specialists. The investigation determined that an unauthorized actor accessed our AWS environment at various periods of time between February 26, 2026 and March 13, 2026, and that during that period of unauthorized access, certain information contained within AWS was viewed or copied by the unknown actor. Pivot Health therefore undertook a comprehensive review of the data at risk to determine what information was potentially affected, and to whom that information related. Those efforts recently completed, and Pivot Health proceeded with notifying impacted individuals by written letter.

What Information Was Involved? While the notice letter received by notified individuals will specify what particular data elements were impacted for them, generally speaking, the review of the involved data demonstrated that the following types of information were present in the impacted files: names, dates of birth, health insurance information, including health insurance billing and payment information, identification numbers such as member identification, person identification, certificate identification and coverage identification, and dates of coverage, and in some cases, financial account information. At this time, we are unaware of any identity theft or fraud occurring as a result of this event.

What We Are Doing. The confidentiality, privacy, and security of information within our care is among Pivot Health's highest priorities. Upon becoming aware of the suspicious activity, we promptly commenced an investigation to confirm the nature and scope of the event. We are also reviewing existing security policies and have implemented additional cybersecurity measures to further protect against similar events moving forward. We are also notifying potentially impacted individuals, so they may take steps to best protect your information, should they feel it is appropriate to do so.

For More Information. Potentially affected individuals may have questions regarding this incident that are not addressed in this notice. If you have additional questions and believe you may be impacted by this incident, please call the dedicated toll-free assistance line at 844-593-8519 Monday to Friday, from 8:00 am to 8:00 pm EST, excluding U.S. holidays. You may also write to Pivot Health at 401 North Miami Avenue Suite 205, Miami, Florida, 33127.

What You Can Do. While Pivot Health is not aware of any identity theft or fraud occurring as a result of this incident, Pivot Health nonetheless encourages potentially affected individuals to remain vigilant against incidents of identity theft and fraud by reviewing their account statements and to monitor their credit reports for suspicious activity. 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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals 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 one-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 an individual is a victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should an individual 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 a consumer's name without their consent. However, individuals should be aware that using a credit freeze to take control over who gets access to the personal and financial information in a 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, individuals cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals 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 they are a victim of identity theft.

Should individuals 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/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, P.O. Box 160, Woodlyn, PA 19094

Individuals 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 reporting bureaus, the Federal Trade Commission, or their 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. Individuals can obtain further information on how to file such a complaint by way of the contact information listed above. Individuals 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, individuals 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 appropriate state Attorney General. This notice has not been delayed by law enforcement.