

Persante Health Care Notifies Individuals of Data Security Incident

Mt. Laurel Township, New Jersey – November 26, 2025 – Persante Health Care is providing notice of a recent data security incident that may have involved personal and/or protected health information. Persante Health Care is a national provider of sleep and balance center management services for numerous medical facilities. Persante Health Care takes the privacy and security of all information within its possession very seriously. Persante Health Care has sent notice of this incident to potentially affected individuals and provided resources to assist them.

On or about January 28, 2025, Persante Health Care became aware of unusual activity in its network. Upon discovering this activity, Persante Health Care immediately took steps to secure the network and launched an investigation with the support of external cybersecurity experts to learn more about the scope of the incident and any impact to data. Through that investigation, Persante Health Care learned of information suggesting that an unknown actor gained unauthorized access to its network between January 23 and 28, 2025 and potentially accessed or acquired certain files, some of which may have contained individuals' personal and/or protected health information. Persante Health Care undertook a comprehensive review of the potentially impacted data and, on or about October 3, 2025, determined that certain individuals' personal and/or protected health information may have been involved. Persante Health Care then worked to notify affected medical facilities and coordinated notification efforts with those providers and verified the affected information and mailing addresses for impacted individuals to effectuate formal notification.

The personal and protected health information that may have been involved in the incident included: names, dates of birth, Social Security numbers, driver's license numbers, state identification numbers, passport numbers, governmental identification numbers, Individual Taxpayer Identification Numbers, dates of medical service, physician or medical facility information, medical condition or treatment information, medical diagnosis information, Medicare or Medicaid numbers, individual health insurance policy numbers, financial account numbers, payment card numbers, patient account numbers, medical record numbers, medical device identifiers, and biometric identifiers.

As soon as it discovered the incident, Persante Health Care took the steps referenced above. Persante Health Care also notified the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold the responsible parties accountable, if possible. Persante Health Care takes the security and privacy of personal and protected health information in its possession very seriously and has taken additional steps to prevent a similar event from occurring in the future.

On November 26, 2025, Persante Health Care mailed notice of this incident to potentially affected individuals for which Persante Health Care had identifiable address information. In notification letters, Persante Health Care provided information about the incident and steps that potentially affected individuals can take to protect their information.

Persante Health Care has established a toll-free call center to answer questions about the incident and to address related concerns. Call center representatives are available Monday through Friday between 9:00 a.m. to 6:30 p.m. Eastern Time and can be reached at (844) 354-1778.

The privacy and protection of personal and protected health information is a top priority for Persante Health Care. We deeply regret any concern this incident may cause.

We are providing the following information to help those who want to know more about steps they can take to protect themselves and their personal information:

What steps can I take to protect my personal information?

- Please notify your financial institution immediately if you detect any suspicious activity on any of your accounts, including unauthorized transactions or new accounts opened in your name that you do not recognize. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities.
- You can request a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To do so, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is listed at the bottom of this page.
- You can take steps recommended by the Federal Trade Commission to protect yourself from identity theft. The FTC's website offers helpful information at ftc.gov/idtheft.
- Additional information on what you can do to better protect yourself is included in your notification letter.

How do I obtain a copy of my credit report?

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228, 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. Use the following contact information for the three nationwide credit reporting agencies:

Equifax	Experian	TransUnion
P.O. Box 105851	P.O. Box 9532	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-833-799-5355
www.equifax.com	www.experian.com	www.transunion.com/get-credit-report

How do I put a fraud alert on my account?

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 one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com. For TransUnion: www.transunion.com/fraud-alerts.

How do I put a security freeze on my credit reports?

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. You may make that request by certified mail, overnight mail, or regular stamped mail, or online by following the instructions found at the websites listed below. You will need to provide the following information when requesting a security freeze (note that if you are making a request for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) address. You may also be asked to provide other personal information such as your email address, a copy of a government-issued identification card, and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address,

and the date of issue. There is no charge to place, lift, or remove a freeze. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
1-800-685-1111
www.equifax.com

Experian Security Freeze
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion (FVAD)
PO Box 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com/credit-freeze

What should I do if my family member was involved in the incident and is deceased?

You may choose to notify the three major credit bureaus, Equifax, Experian and Trans Union, and request they flag the deceased credit file. This will prevent the credit file information from being used to open credit. To make this request, mail a copy of your family member's death certificate to each company at the addresses below.

Equifax

Experian

TransUnion

Equifax Information Services

Experian Information Services

Transunion Information Services

P.O. Box 740256

P.O. Box 9701

P.O. Box 2000

Atlanta, GA 30374

Allen, TX 75013

Chester, PA 19016

What should I do if my minor child or protected person's information was involved in the incident?

You can request that each of the three national credit reporting agencies perform a manual search for a minor's or protected person's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of a minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>. Contact information for the three credit reporting agencies may be found above.