

DAP Health, Inc.  
c/o Cyberscout  
PO Box 1286  
Dearborn, MI 48120-9998



Via First-Class Mail



December 26, 2024

## Notice of Data Breach

Dear [REDACTED]:

DAP Health, Inc., along with its subsidiary Borrego Health (collectively “DAP Health” or “we”) write to inform you of a recent event that may impact some of your personal information. DAP Health takes this event seriously and the privacy, security, and confidentiality of information in our care is among our highest priorities. While DAP Health is not aware of any actual or attempted misuse of your information to perpetrate financial fraud, out of an abundance of caution, we are providing you with an overview of the event, our response, and resources to help further protect your information, should you feel it necessary to do so.

### What Happened?

On July 22, 2024, DAP Health detected suspicious activity in its email environment. Upon discovery of this event, DAP Health promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the event. As a result of the investigation, DAP Health learned that an unauthorized actor accessed and/or acquired certain files and data stored within its email environment.

Upon learning this, DAP Health began a time-consuming and detailed reconstruction and review of the data stored on their email environment at the time of this event, to understand whose information was affected. On November 26, 2024, DAP Health identified those persons whose sensitive data was included within the impacted data.

### What Information Was Involved?

As part of its normal business operations, DAP Health collected certain information from its employees, patients, and clients. To that end, and as a result of DAP Health’s investigation, DAP Health determined that the information related to you that may have been acquired without authorization as a result of the event consists of your: [REDACTED]

### What We Are Doing?

The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon becoming aware of the event, we moved promptly to investigate and respond to the event and notify potentially affected individuals. We are notifying potentially affected individuals, including you, so that you may take further steps to best protect your information, should you feel it is necessary to do so. As an added precaution, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file.

0000102G0500

P

This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company, specializing in fraud assistance and remediation services. While DAP Health is covering the cost of these services, you will need to complete the activation process yourself.

**What You Can Do.**

You can learn more about how to help protect yourself against potential information misuse in the enclosed *Steps You Can Take To Help Protect Personal Information*. There, you will find instructions on how to activate in the complimentary credit monitoring. We also encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and credits reports for suspicious activity, and to report any suspicious activity promptly to your bank, credit card company, or other applicable institution.

To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED] Please note that the code is case-sensitive and will need to be entered as it appears.

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Once enrolled you will have twelve (12) months of monitoring services. At the end of twelve (12) months, the services will be deactivated. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

**For More Information.**

We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line at **833-799-4324**, Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time, excluding major U.S. holidays. Please have this letter ready if you call.

Sincerely,

DAP Health, Inc.

## Steps You Can Take To Help Protect Personal Information

### Monitor Your Accounts

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](http://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, 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:

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

| <b>Equifax</b>  | <b>Experian</b>   | <b>TransUnion</b>   |
|---|---|---|
| <a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a> | <a href="https://www.experian.com/help/">https://www.experian.com/help/</a> | <a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a> |
| 1-888-298-0045  | 1-888-397-3742  | 1-800-916-8800  |
| Equifax Fraud Alert, P.O. Box 105069<br>Atlanta, GA 30348-5069  | Experian Fraud Alert, P.O. Box<br>9554,<br>Allen, TX 75013                  | TransUnion Fraud Alert, P.O. Box<br>2000, Chester, PA 19016                                 |
| Equifax Credit Freeze, P.O. Box<br>105788 Atlanta, GA 30348-5788  | Experian Credit Freeze,<br>P.O. Box 9554, Allen, TX<br>75013                | TransUnion Credit Freeze, P.O. Box<br>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 your 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, D.C. 20580; [www.identitytheft.gov](http://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, DC 20001; 1-202-727-3400; and [oag.dc.gov](http://oag.dc.gov).

*For Maryland residents*, the Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. DAP Health is located at 1695 N Sunrise Way, Palm Springs, CA 92262 and can be reached at (760) 323-2118.

*For New York residents*, the New York Department of State Division of Consumer Protection, Once Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 51-8-474-8553 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and New York's Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>

*For North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and [www.ncdoj.gov](http://www.ncdoj.gov).

*For New Mexico residents*, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

*For Rhode Island residents*, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and [www.riag.ri.gov](http://www.riag.ri.gov). Under Rhode Island law, you have the right to obtain any police report filed in regard to this event. This event involves 1 individual in Rhode Island.