

Dove Healthcare
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



To the Legal Representative of:



IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear Legal Representative of: [REDACTED]:

I am writing with important information regarding a recent data security incident at Dove Healthcare. The privacy and security of the protected personal information entrusted to us is of the utmost importance. As such, we wanted to provide you with information about the incident, explain the services we are making available to your legal ward, and let you know that we continue to take significant measures to protect their information.

What Happened?

We experienced a security incident on or about July 6, 2024 that impacted our network.

What We Are Doing.

Upon learning of the issue, we commenced a prompt and thorough investigation. As part of our investigation, we notified federal law enforcement of the incident, engaged external cybersecurity experts and conducted a manual review, and based on that review we discovered on March 6, 2025 that certain files containing your legal ward's protected personal information were subject to unauthorized access or acquisition. We want to make you aware of the incident and provide you with steps you can take to further protect their information.

Additionally, Dove Healthcare is reviewing its existing policies and training protocols relating to data protection while enhancing security measures and monitoring tools to further mitigate risks of this nature. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of the wards' protected personal information.

What Information Was Involved?

The potentially impacted files may have contained the legal ward's



What You Can Do.

We have no evidence that any of your legal ward's information has been used for identity theft or to commit financial fraud. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. We are also providing them with complimentary 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 months from the date of enrollment when changes occur to your credit file. You have until [REDACTED] to enroll. This notification is sent to you the same day that the change or update takes place with the bureau. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

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].

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. 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.

This letter also provides other precautionary measures to protect their personal information, including placing a fraud alert and/or security freeze on their credit files and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing their financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of protected personal information in our possession and have taken precautions to safeguard it. We continually evaluate and modify our practices and controls to enhance the security and privacy of your legal ward's personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED]. Representatives are available from 8:00 am to 8:00 pm Eastern Time, Monday through Friday, excluding holidays. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against potential misuse of their information.

Sincerely,

Dove Healthcare

- OTHER IMPORTANT INFORMATION -

1. **Placing a Fraud Alert.**

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial 90-day “Fraud Alert” on the credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms the fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289



2. **Consider Placing a Security Freeze on Your Credit File.**

If you are very concerned about your ward becoming a victim of fraud or identity theft, you may request a “security freeze” be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing the credit report or any information from it without your express authorization. You may place a security freeze on their credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you will need to supply your and your ward’s name, address, date of birth, Social Security number, and other personal information. After receiving the freeze request, each credit reporting company will send a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze the credit file.

3. **Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. **Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts.

- You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338) or TTY: 1-866-653-4261, or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

You may also reach out to the Social Security Administration to notify them of the impact on your Social Security Number. They may be reached via the telephone by contacting the National 800 Number at 1-800-772-1213 between 8:00 a.m. - 7:00 p.m. Eastern Time, Monday through Friday. If you are deaf or hard of hearing and use TTY equipment, you can call the TTY number at 1-800-325-0778.

5. Protecting Your Medical Information.

We have no information to date indicating that the medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect your legal ward from medical identity theft.

- Only share the health insurance cards with your health care providers and other family members who are covered under the insurance plan or who help with your medical care.
- Review the "explanation of benefits statement" which you receive from your health insurance company. Follow up with the insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask the insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with the insurance company or the care provider for any items you do not recognize.

7. State Specific Information.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA) which include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), or TTY: 1-866-653-4261.



