



1900 M Street NW, Suite 250
Washington, DC 20036

Phone: (202) 296-3585
Website: www.zwillgen.com

Marci Rozen
(202) 706-5226
marci@zwillgen.com

August 13, 2026

Via Online Submission

Attorney General Mike Hilgers
Attorney General's Office
1445 K Street, Room 2115
Lincoln, NE 68508

Re: Notice of Data Security Incident

Dear Attorney General Hilgers:

ZwillGen represents *Terry J. Dubrow, MD, A Medical Corporation* (the “Practice”) in connection with the recent data security incident described below. The purpose of this letter is to notify you of the incident and provide you with a copy of the notice sent to impacted residents.

1. Nature of the Security Incident

On May 30, 2026, The Practice was contacted by an unauthorized actor who claimed to have gained access to some of its digital systems. Upon learning of this claim, the Practice immediately took steps to secure its systems and engaged forensic experts to investigate. The investigation determined that an unauthorized actor accessed a portion of the Practice’s network beginning on January 16, 2025, and acquired certain data the Practice maintains. The Practice then conducted a prompt review of the data involved to assess what information was impacted and to identify the individuals whose information was contained in the acquired files. On July 27, 2026, the Practice learned that certain patient personal information was accessed and acquired without authorization.

At this time, the Practice has no evidence that any impacted individuals’ personal information has been misused or publicly disclosed. Based on the investigation to date, the Practice believes the incident has been contained. While no organization can eliminate all future risk, the Practice is notifying individuals out of an abundance of caution and in accordance with its legal obligations.

The affected information varies by individual but may include individuals’ names, driver’s license or state ID number, phone number, mailing address, email address, Social Security Number, date of birth, and/or medical information (including, prescription information, treatment information, procedure images, and x-rays).

2. Number of Nebraska Residents Affected

On August 13, 2026, the Practice notified fourteen (14) Nebraska residents of this incident via first class U.S. mail. A sample copy of the notification letter sent to impacted individuals is included with this correspondence.

3. Steps Taken in Response to the Incident

As noted above, the Practice conducted a thorough investigation with the assistance of forensic experts and promptly secured its systems. It took steps to prevent further disclosure of the data and continues to implement additional measures to enhance the security of its systems. The Practice also reported the incident to the Federal Bureau of Investigation.

Out of an abundance of caution, the Practice has provided individuals with information about steps they can take to protect their personal information and has offered individuals the chance to enroll in complimentary identity protection services through IDX.

4. Contact Information

The Practice remains dedicated to protecting the information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at 202-706-5226 or via email at marci@zwillgen.com.

Sincerely,

A handwritten signature in black ink that reads "Marci Rozen". The signature is written in a cursive, flowing style.

Marci Rozen

Encls: Sample Consumer Notification Letter

cc: Jamie Elbert, jamie.elbert@zwillgen.com



Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>
Enrollment Deadline: November 13, 2026
To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

August 13, 2026

Subject: Notice of Data <<Variable Text : Header>>

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of a data security incident *Terry J. Dubrow, MD, A Medical Corporation* (the “Practice”) recently experienced. Please read this letter carefully, as this incident impacted some of your information. This letter is to notify you of the incident, offer you complimentary identity protection services, and inform you about steps you can take to help protect your personal information.

What Happened. The Practice was recently contacted by an unauthorized actor who claimed to have gained access to some of the systems in our digital environment. Upon learning of this claim, we immediately took steps to secure our systems and engaged forensic experts to investigate. The investigation determined that an unauthorized actor accessed a portion of our network beginning on January 16, 2025, and acquired certain data we maintain. We then conducted a prompt review of the data involved to assess what information was impacted and to identify the individuals whose information was contained in the acquired files. On July 27, 2026, the Practice learned that some of your personal information was accessed and acquired without authorization. At this time, we have no evidence that your personal information has been misused or publicly disclosed. Based on our investigation to date, we believe the incident has been contained. While no organization can eliminate all future risk, we are notifying you out of an abundance of caution and in accordance with our legal obligations.

What Information Was Involved. The data that was acquired included your name and information contained in your patient chart that you or your referring physician provided the Practice. That information would have contained, to the extent provided, your driver’s license or state ID number, phone number, mailing address, email address, Social Security Number, and medical information (including date of birth, prescription information, treatment information, procedure images, and x-rays).

What We Are Doing. As noted above, we conducted a thorough investigation with the assistance of forensic experts and promptly secured our systems. We took steps to prevent further disclosure of the data and continue to implement additional measures to enhance the security of our systems. We also reported the incident to the Federal Bureau of Investigation. Out of an abundance of caution, we are providing you with information about steps that you can take to help protect your personal information and are offering you <<12/24>> months of complimentary identity protection services from IDX at no charge to you. These services help detect possible misuse of your information and provide you with identity protection support.

What You Can Do. You can follow the recommendations included with this letter to help protect your information. In addition, you can enroll in IDX’s complimentary identity protection services by visiting <https://app.idx.us/account-creation/protect>

or calling 1-888-201-6003. When enrolling, please provide the following unique code: <<ENROLLMENT>>. Please note that you must be at least 18 years of age to enroll in these services.

For More Information. For more information about how you can protect your information, please review the resources on the following page. If you have questions regarding the incident, please call 1-888-201-6003, Monday through Friday, 6:00AM to 6:00PM Pacific Time, excluding holidays.

The security of your information is a top priority for us. We take your trust in us and this matter very seriously, and we regret any worry or inconvenience that this may cause you.

Sincerely,

Terry J. Dubrow, MD, A Medical Corporation
1617 Westcliff Dr.
Newport Beach, CA 92660

Additional Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the “FTC”).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com/, calling toll-free 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. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com/get-credit-report

Fraud Alert: 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.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. For TransUnion: www.transunion.com/credit-freeze.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission 600

Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
<https://oag.maryland.gov>
888-743-0023

Oregon Attorney General

1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General

The Capitol
Albany, NY 12224
ag.ny.gov
800-771-7755

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

**NY Bureau of Internet and
Technology**
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

<<RI Specific Language>>