

Jennifer Archie
Direct Dial: 202-637-2205
jennifer.archie@lw.com

555 Eleventh Street, N.W., Suite 1000
Washington, D.C. 20004-1304
Tel: +1.202.637.2200 Fax: +1.202.637.2201
www.lw.com

LATHAM & WATKINS LLP

FIRM / AFFILIATE OFFICES

Austin	Milan
Beijing	Munich
Boston	New York
Brussels	Orange County
Century City	Paris
Chicago	Riyadh
Dubai	San Diego
Düsseldorf	San Francisco
Frankfurt	Seoul
Hamburg	Silicon Valley
Hong Kong	Singapore
Houston	Tel Aviv
London	Tokyo
Los Angeles	Washington, D.C.
Madrid	

August 9, 2024

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
State of Maryland
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

RE: Notice of Data Security Incident

Dear Attorney General:

I am writing on behalf of MD Now Medical Centers, Inc. (“MD Now”) to provide you with information about a recent data security incident involving the personal information of Maryland patients and employees (the “Incident”).

MD Now operates urgent care centers in Florida and has been affiliated with HCA Florida Healthcare since January 2022. MD Now learned of the Incident on May 20, 2024, and quickly confirmed that it involved an isolated and legacy IT system that was used to support MD Now’s operations prior to its affiliation with HCA Florida Healthcare. Fortunately, the Incident did not involve any IT systems that MD Now currently uses to provide care to its patients or to support its general business operations. We have identified one (1) Maryland resident whose HR information was impacted by the Incident.

MD Now retained counsel and forensic experts immediately after learning about the Incident, in order to contain and assess its impact. The investigation determined that data was removed from two servers, one that stored copies of faxes of discharge and prescription forms provided to patients who visited MD Now clinics before August 2023, and another which included legacy HR records such as employee onboarding and termination papers that contained information about MD Now’s current or previous employees, and in some instances, their dependents or beneficiaries. The external vendor completed an expedited data mining analysis on July 15, 2024, allowing MD Now to identify impacted individuals and the specific data elements

LATHAM & WATKINS LLP

impacted (for each). Addresses were located and appended as needed, and IDX is mailing notice letters on or about August 9, 2024. A copy of the notification letter for the affected individual is attached to this letter as **Exhibit A**.

If you need any further information about the Incident in the meantime, please contact me at (202) 637-2205 or jennifer.archie@lw.com.

Respectfully submitted,

A handwritten signature in blue ink, appearing to read "Jennifer C. Archie". The signature is fluid and cursive, with the first name "Jennifer" being more prominent.

Jennifer C. Archie
Of LATHAM & WATKINS LLP

EXHIBIT A



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

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

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://response.idx.us/mdnow>

August 9, 2024

Re: Notice of Data Breach

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

We are writing to provide you (or your parent or guardian) with information about a recent criminal cybersecurity attack involving your personal information and/or the personal information of your dependent or beneficiary. The purpose of this notice is to help you understand what information may have been involved in the cybersecurity attack and to provide you with information about the steps you can take to protect your privacy, including the enrollment in two years of free credit monitoring and identity theft protection services. Please take the time to carefully read the sections below entitled “What You Can Do” and “Steps You Can Take to Help Protect Your Information.”

Who is MD Now Urgent Care? MD Now Urgent Care (“MD Now”) operates urgent care clinics in Florida, and our records indicate that you currently are, or previously were, employed by MD Now or that you are a dependent or beneficiary of someone who is, or was, employed by MD Now. For more information about MD Now or the location of our clinics, please visit <https://www.mymdnow.com/>. You may also call the toll-free number below for more information.

What Happened? On May 20, 2024, MD Now discovered a criminal cybersecurity attack on one of its IT systems and immediately retained forensic experts to investigate the attack. The investigation determined that an unknown and unauthorized criminal accessed the system and removed certain documents earlier in May, including information about current and former MD Now employees and their dependents and beneficiaries, such as MD Now employee onboarding and termination documents. MD Now reported the attack to law enforcement authorities.

What Information is Involved? The investigation allowed us to determine that the following of your information was accessed during the attack: name, <<ELEMENTS_FOUND>>.

What is MD Now Doing? MD Now immediately retained forensic, threat-intelligence and other IT experts and advisors, who worked to investigate and to contain the attack, including by implementing additional security measures. MD Now is not aware of any of the information accessed during the attack being used by the criminal responsible for the attack or being made available to others on the internet or dark web. Despite that and to help alleviate any concerns you may have, MD Now is offering you free credit monitoring and identity protection services provided by IDX for a period of two years. The services include credit monitoring, a \$1,000,000 insurance reimbursement policy and identity restoration, in the event that you are a victim of identity theft, and dark web monitoring to identify any of your information that is made available through illegal online forums. To activate the services, please follow the instructions included in the attached “Steps You Can Take to Help Protect Your Information.”

What You Can Do. You should continue to be vigilant about identity theft and fraud – please review your account and financial statements and monitor available credit reports for unauthorized or suspicious activity. You should also be careful when responding to any text, email, telephone or other requests for your personal or sensitive information. MD Now will never request your personal or sensitive information by text, email or telephone. Finally, you should never open links or attachments sent from unknown or suspicious sources. Additional information is provided in the attached *“Steps You Can Take to Help Protect Your Information.”*

Who You Can Call. For further information, please call 1-888-737-9707, Monday to Friday from 9 am – 9 pm Eastern Time.

Sincerely,

MD Now

Steps You Can Take to Help Protect Your Information

Enroll in IDX Credit Monitoring and Identity Protection Services

Go to <https://response.idx.us/mdnow> and follow the instructions to enroll in the identity protection services being provided by IDX. Your person Enrollment Code is provided at the top of this letter. Please note the deadline to enroll is November 9, 2024.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 with the credit reporting bureau. 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

If you discover any suspicious items on your credit reports or from the fraud alert and have enrolled in IDX identity protection services, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of the IDX ID Care Team who will help you determine the cause of the suspicious items. In the event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, free of charge, 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you 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, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency filed by you concerning identity theft if you are a victim of identity theft.

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

Equifax	Experian	TransUnion
https://www.equifax.com/	https://www.experian.com/	https://www.transunion.com/
1-888-378-4329	1-888-397-3742	1-800-916-8800
Equifax Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374	Experian Fraud Center P.O. Box 9554 Allen, TX 75013	TransUnion Fraud Victim Assistance Department 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	Experian Credit Freeze P.O. Box 9554 Allen, TX 75013

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud (this letter alone does not suggest that you are a victim of or at risk of identity theft or fraud). Please note that in order for you to file a police report for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Florida residents, the Florida Attorney General can be contacted at PL-01, The Capitol, Tallahassee, FL 32399-1050, <https://www.myfloridalegal.com/>, 850-414-3300.

For California residents, the California Office of Privacy Protection (www.oag.ca.gov/privacy) may be contacted for additional information on protection against identity theft. The California Attorney General can be contacted at 1300 I Street, Sacramento, CA 95814, www.oag.ca.gov, 800-952-5225.

For Maryland residents, the Maryland Attorney General can be contacted at 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 410-576-6300.

For North Carolina residents, the North Carolina Attorney General can be contacted at Consumer Protection Division, Mail Service Center 9001, Raleigh, NC 27699, www.ncdoj.gov, 877-566-7226.

For Rhode Island residents, the Rhode Island Attorney General can be contacted at 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400. You have the right to file or obtain a police report regarding this incident.

For District of Columbia residents, the District of Columbia Attorney General can be contacted at 400 6th Street NW, Washington, DC 20001, www.oag.dc.gov, 202-727-3400.

For Iowa residents, the Iowa Attorney General can be contacted at 1305 E. Walnut Street, Des Moines, Iowa 50319, <https://www.iowaattorneygeneral.gov/>, 515-281-5926 or 888-777-4590.

For New York residents, the New York Attorney General may be contacted at the Capital, Albany, NY 12224, www.ag.ny.gov, 800-771-7755.

For Oregon residents, the Oregon Attorney General may be reached at 1162 Court Street NE, Salem, OR 97301, <https://www.doj.state.or.us>, 503-378-4400.

For South Carolina residents, the South Carolina Department of Consumer Affairs may be reached at 293 Greystone Blvd., Ste. 400, Columbia, SC 29210, www.consumer.sc.gov, 800-922-1594.

For Kentucky residents, the Kentucky Attorney General may be contacted at 700 Capital Avenue, Suite 118, Frankfurt, KY 40601, www.ag.ky.gov, 502-696-5300.

For Massachusetts residents, You have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-2200, <https://www.mass.gov/contact-the-attorney-generals-office>.

For New Mexico residents, you have the right to obtain a police report regarding 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. 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 agencies 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 a 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>, or by writing to the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.