mwe.com

Edward Zacharias
Attorney at Law
ezacharias@mwe.com
+1 617 535 4018

November 15, 2024

VIA EMAIL

Attorney General Raúl R. Labrador
Idaho Office of the Attorney General
Consumer Protection Division
P.O. Box 83720
Boise, ID 83720-0010
consumer_protection@ag.idaho.gov

RE: athenahealth, Inc. – Incident Notification

Dear Attorney General Labrador:

McDermott, Will & Emery LLP, in its capacity as counsel for athenahealth, Inc. ("athenahealth"), is writing to provide courtesy notification on behalf of athenahealth of an incident that affected the security of personal information of approximately one Idaho resident, as discussed in further detail below. athenahealth is providing this notification on behalf of certain HIPAA covered entities to which athenahealth acts as a business associate and that provided athenahealth with the data impacted by this incident. In providing this courtesy notification, athenahealth does not waive any potentially applicable rights or defenses, including but not limited to those regarding the applicability of Idaho law.

athenahealth notified the Department of Health and Human Services, Office for Civil Rights of this incident on November 15, 2024, consistent with applicable HIPAA reporting obligations and procedures. Affected individuals were notified of this incident and the impact to their personal information on November 15, 2024 pursuant to the enclosed template; as part of that notification, affected individuals were provided with identity protection services at no cost and consistent with applicable law and legal requirements.

As part of this submission, we are providing a summary of the incident, the scope of information involved, and the remedial measures athenahealth has taken to mitigate the potential impact of this situation.

Summary of what happened:

athenahealth is an electronic health record and revenue cycle management vendor to medical provider organizations across the country. As part of its service offering, athenahealth submits patient insurance eligibility queries, and receives insurance provider responses, on behalf of healthcare providers (collectively, "Eligibility Transaction Files"). On September 16, 2024, athenahealth was notified by an insurance provider that certain Eligibility Transaction Files were visible through a publicly accessible internet repository. Upon learning of this issue, athenahealth immediately removed the files and information from the repository and promptly began an investigation into how this situation occurred. Upon review, athenahealth determined the root cause was a one-

time, manual error in the way an athenahealth employee configured the repository that resulted in the inadvertant upload of the Eligibility Transaction Files.

Scope of information involved:

While the information contained in the Eligibility Transaction Files was not the same for everyone affected, there were certain common demographic data elements, such as the individual's name, address, insurance member ID, date of birth, and gender, as well as certain clinical information such as their healthcare provider's name, their healthcare insurance provider organization and, potentially, additional information regarding their clinical care and payment responsibilities for that care (e.g., co-payment amounts) – if that information was included within an insurance provider's response to the eligibility query. Importantly, no financial information such as credit card or financial account numbers were included in the Eligibility Transaction Files.

Steps taken to mitigate the potential impact of this situation:

As mentioned above, athenahealth took swift action to remove the Eligibility Transaction Files from the repository on the same day it learned of this issue. athenahealth has also taken certain steps to prevent a future similar occurrence, and it is currently evaluating additional safeguards, workflows, and process improvements. Corrective action was imposed on the employee responsible for the unauthorized disclosure, and additional training has been provided to that employe on the importance of information security and protecting the integrity and confidentiality of sensitive information.

To date, athenahealth is not aware of any misuse of the Eligibility Exchange Files or any information contained therein. Nor is athenahealth aware of any reports of identity theft or fraud stemming from this incident. Nevertheless, and out of an abundance of caution, athenahealth has provided complimentary access to identity protection services through Experian to affected individuals, as well as provided additional information about the process for placing fraud alerts and/or security freezes on their credit cards and obtaining free credit reports.

athenahealth takes the privacy and security of patient information very seriously, and it is committed to taking appropriate steps to ensure something like this does not happen again. While athenahealth has confirmed the root cause of this issue was attributable to an individual's manual error – and not the product of technical or system malfunction – athenahealth continues to evaluate opportunities to enhance its information security capabilities and protocols to further protect the security and confidentiality of sensitive information under its control. Should you have any questions regarding this notification, please feel free to contact me at your convenience.

Sincerely,

Edward Zacharias
Cc: Karinna Allen, Chief Compliance Officer athenahealth, Inc.

athenahealth
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

November 15, 2024

M3892-L02-0000002 T00001 P001 ********SCH 5-DIGIT 12345
PARENT OR GUARDIAN OF FOR MINOR RECS
SAMPLE A SAMPLE - L02
APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY

[Notice of Data Breach for CA]

Dear Sample A. Sample

athenahealth, Inc. ("athenahealth"), an electronic health record and revenue cycle management vendor to your medical provider organization [Company], is writing to inform you of an incident impacting some of your personal information. athenahealth values your privacy and we apologize for any inconvenience or concern this issue may have caused. While we have no reason to believe your information has been misused in any way, we want you to understand how this occurred and the steps we have taken to address the situation, including offering 12 months of identity protection services to you at no cost as explained more fully below.

Summary of what happened: As part of its service offering, athenahealth submits and receives patient insurance eligibility queries and insurance provider responses on behalf of healthcare providers (collectively, "Eligibility Transaction Files"). On September 16, 2024, athenahealth was notified by an insurance provider that certain Eligibility Transaction Files were visible through a publicly accessible internet repository. Upon learning of this issue, we immediately removed the files and information from the repository and promptly began an investigation into how this situation occurred. Upon review, we determined the root cause was a one-time, manual error in the way the repository was configured that resulted in the inadvertant upload of the Eligibility Transaction Files. We believe the Eligibility Transaction Files were uploaded to the repository sometime on or after April 3, 2024.

What information was involved: While the information contained in the Eligibility Transaction Files was not the same for everyone affected, it generally included certain demographic information, such as your name, address, insurance member ID, date of birth and gender, as well as certain clinical information such as your healthcare provider's name, your healthcare insurance provider organization and, potentially, additional information regarding your clinical care and payment responsibilities for that care (i.e., co-payment amounts) – if that information was included within your insurance provider's response to the eligibility query. Importantly, neither your Social Security number nor sensitive financial information such as credit card or financial account numbers were included in the Eligibility Transaction Files.

What is athenahealth doing to address the situation: As mentioned above, we took swift action to remove the Eligibility Transaction Files from the repository on the same day we learned of this issue. We are also evaluating

additional safeguards, workflows, and process requirements to prevent a similar future occurrence, in addition to providing training and education to the individual responsible for the configuration error.

What can you do: While we have no reason to believe that any of your information has been misused, out of an abundance of caution, and to help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for 12 months at no cost.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** August 23, 2025 (your code will not work after this date)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/RR1Bplus
- Provide your **activation code:** ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-833-931-7577 by August 23, 2025. Be prepared to provide engagement number B128630 as proof of eligibility for the Identity Restoration services by Experian.

VARIABLE PARAGRAPH FOR MINOR

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE^{TM}:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

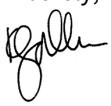
- **Lost Wallet:** Provides assistance with canceling/replacing lost or stolen credit, debit, and medical cards.
- **Child Monitoring:** For 10 children up to 18 years old, Internet Surveillance and monitoring to determine whether enrolled minors in your household have an Experian credit report available. Also included are Identity Restoration and up to $1M Identity Theft Insurance.**

VARIABLE PARAGRAPH FOR CA

athenahealth takes the privacy and security of patient information very seriously, and we are committed to taking appropriate steps to ensure something like this does not happen again. While we believe it is a remote risk that the disclosure will result in any potential harm, out of an abundance of caution, we recommend that you look for any suspicious activity as it relates to payment for your healthcare treatment.

We regret any inconvenience or concern this issue may cause. If you have any questions, please do not hesitate to contact athenahealth at ETF.Support@athenahealth.com.

Sincerely,



Karinna Allen
Chief Compliance Officer
athenahealth, Inc.
80 Guest Street | Boston, MA 02135

*Offline members will be eligible to call for additional reports quarterly after enrolling.
** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
(800) 525-6285	(888) 397-3742	(800) 916-8800

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as indicated above.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the respective address indicated above.

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report.

If you are a Connecticut resident, you may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

If you are a District of Columbia resident, you may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 1-202-727- 3400, www.oag.dc.gov.

If you are a Kentucky resident, you can obtain information about steps you may take to avoid identity theft from following sources: the FTC (see contact information above), the major consumer credit reporting agencies (see contact information above), and the Office of the Kentucky Attorney General: 700 Capital Avenue, Suite 118, Frankfort, KY 40601-3449, www.ag.ky.gov, 1-888- 432-9257.

If you are a Maryland resident, you can contact the Maryland Office of the Attorney General, Consumer Protection Division at: 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023.

If you are a Massachusetts resident, under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. 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, 1-617-727-8400, www.mass.gov/contact-the-attorney-generals-office.

If you are a New York resident, you can contact the New York Office of the Attorney General at www.ag.ny.gov, 1- 800-771-7755; the New York Department of State, www.dos.ny.gov, 1-800-697-1220; and the New York Division of State Police, www.ny.gov/agencies/division-state-police, (914) 834-9111.

If you are a North Carolina resident, you can contact the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, https://ncdoj.gov, 1-877-566-7226.

If you are an Oregon resident, state law advises you to report any suspected identity theft to law enforcement or to the FTC.

If you are a Rhode Island resident, you have the right to obtain a police report. You also have the right to request a security freeze, as described above. You can also contact the Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, (401) 274-4400 or file a police report by contacting (401) 444-1000.

If you are a West Virginia resident, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.