SECURITY BREACH NOTIFICATION FORM

Delaware Department of Justice
Consumer Protection Unit
820 N. French Street
Wilmington, DE 19801
security.breach.notification@state.de.us

Type of Report
◉ Initial Breach Report
○ Addendum to Previous Report

Entity That Owns or Licenses the Computerized Data Whose Security Was Breached					
Name:	AmeriHealth Caritas Delaware				
Street Address:	220 Continental Drive, Suite 300				
City:	Newark	State:	DE	ZIP Code:	19713

Submitted By					
Name:	Gregory T. Parks	Title:	Partner		
Firm (*if different*):	Morgan Lewis				
Street Address:	1701 Market Street				
City:	Philadelphia	State:	PA	ZIP Code:	19103
Telephone:	215-963-5170	Email:	gregory.parks@morganlewis.com		
Relationship to Entity That Was Breached:	Outside Counsel for AmeriHealth Caritas Family of Companies				

Type of Organization		
☐ Charitable/Non-Profit	☐ Educational	☐ Financial Services
☐ Government – Delaware	☐ Government – Outside Delaware	■ Healthcare
☐ Insurance	☐ Retail/Merchant	☐ Utility
■ Other (please describe):	Medicaid Health Insurance Plan	

Type of Personal Information Involved in the Security Breach

Delaware resident's first name or first initial and last name, in combination with 1 or more of the following (mark all that apply):

■ Social Security number	☐ Driver's license number
☐ Federal identification card number	☐ Passport number
☐ Individual taxpayer ID number	☐ Biometric data
☐ Deoxyribonucleic (DNA) profile	☐ Medical history
☐ Medical treatment by a healthcare professional	☐ Diagnosis of mental/physical condition by healthcare professional

☐ Health insurance policy number, subscriber ID number, or any other unique identifier used by health insurer to identify person

☐ Account number, credit card account number, or debit card number, in combination with any required security code, access code, or password that would permit access to a financial account

☐ Username or email address, in combination with password or security question and answer to access online account

Number of Persons Affected	
Delaware Residents Only	1,393
Total (*including Delaware*)	35,967

Dates	
Breach(es) Occurred (*include start/end dates if known*)	11/15/2019
Breach(es) Discovered	11/15/2019
Consumers Notified	1/14/2020

Form of Notice to Affected Persons*	
■ Written	☐ Telephonic
☐ Electronic	☐ Substitute Notice

** Please attach a sample of the notice*

Was Notification Delayed Because of Law Enforcement Request?	
○ Yes	◉ No

Type of Security Breach (*mark all that apply*)

- ☒ Loss or theft of device or media
- ☐ Internal system breach
- ☐ Insider wrongdoing
- ☐ External breach (*hacking, malware, etc.*)
- ☐ Payment card fraud
- ☐ Inadvertent disclosure
- ☐ Improper disposal
- ☐ Other (*please describe*): _____

Was Information Encrypted?

○ Yes ◉ No

Was Encryption Key Acquired?

○ Yes ○ No ◉ N/A

Brief Description of the Security Breach

This Firm represents AmeriHealth Caritas Delaware ("ACDE"), a subsidiary of the AmeriHealth Caritas Family of Companies ("ACFC"), in connection with a situation that ACFC was alerted to on November 15, 2019. On November 15, 2019, an ACFC employee refused to comply with ACFC's request to return or securely destroy the contents of a personal hard drive that the employee wrongfully kept after ACFC demanded return/destruction of it. The employee in question, who has since been terminated, inappropriately downloaded company information, which included ACDE provider data, to a personal hard drive that was installed into company-issued equipment, against company policy. Furthermore, the employee refused to allow ACFC to confirm that the hard drive in question had been wiped clean of any confidential ACFC information. While ACFC does not presently have reason to believe that the employee intended to misuse or re-disclose this information, and no reason to believe that it has been misused or re-disclosed, we are providing you with this notification in an abundance of caution. ACFC is actively working with law enforcement in order to confirm whether they have acquired the hard drive in question and destroyed the ACDE provider data.

In an abundance of caution, ACFC sent notification letters out to the individuals whose personal information may have been accessed. In addition, ACFC is offering a 2-year subscription to Experian IdentityWork's credit monitoring and and identity theft protection services to all affected individuals. Further information about what ACFC has done and what we are recommending to the individuals in question can be found in the enclosed notification letter that ACFC sent to 1,393 Delaware residents via mail on January 14, 2020.

Location of Breached Information

- ☐ Desktop computer
- ☒ Portable/Laptop computer
- ☐ Smartphone
- ☐ Network server
- ☐ Cloud-Based Server
- ☐ Email
- ☒ Other (*please describe*): Hard Drive

Actions Taken in Response to the Security Breach (*mark all that apply*)

- ☐ Added/strengthened data encryption
- ☐ Changed password/strengthened password requirements
- ☐ Created/updated formal written information security plan
- ☐ Implemented new technical safeguards
- ☐ Improved physical security
- ☐ Revised policies and procedures
- ☒ Sanctioned workforce members involved (incl. termination)
- ☐ Trained or retrained workforce members
- ☐ Implemented periodic technical and nontechnical evaluations/risk analyses/penetration tests
- ☐ Revised contracts with business partners, vendors, subcontractors, service providers
- ☐ Changed business partners, vendors, subcontractors, service providers
- ☒ Other (*please describe*): Reviewing existing controls for possible enhancements

Credit Monitoring or Identity Theft Protection Services Offered?

☒ Credit monitoring ☒ Identity theft protection	Duration:	2-year subscription
	Provider:	Experian IdentityWorks
Briefly describe services:	Credit monitoring and identity theft protection	

Law Enforcement Agency Notified of Security Breach?

◉ Yes ○ No	Name of Agency:	Federal Bureau of Investigation
	Contact Name and Number:	SA Garret M. Kerley, (302) 658-4375
	Report Number (*if applicable*):	

Submit Form

AmeriHealth Caritas
200 Stevens Drive
Philadelphia, PA 19113

January 14, 2020

ACFC_Provider_168
For Addressee Only
[Provider name]
[Address 1]
[Address 2]
[City, State Zip]

Re: Personal Information Potentially Compromised

Dear [Provider name]:

We are writing to tell you about a data security incident that may have exposed some of your personal information. While we have no reason to believe that this information has been or will be used inappropriately, we would like to let you know what happened, what information was involved, what we have done to address the situation, and to remind you of what you can do to protect your continued privacy.

What Happened?

Through its network of affiliated companies, the AmeriHealth Caritas Family of Companies ("AmeriHealth Caritas") operates health plans across a number of states. On or about November 15, 2019, we learned that a former AmeriHealth Caritas employee improperly downloaded company confidential information to a personal hard drive. On that day, we contacted him and requested that he surrender the hard drive or co-operate with us to ensure that the contents of the hard drive had been erased, but he refused to do either. We have reason to believe that the downloaded information included files containing personal information of a number of our providers, including you.

What Information Was Involved?

The files on the hard drive may have included personal information about you, including your first and last name and your social security number. To date, we have not received any reports of improper use of any of this information. Nor do we have any reason to believe that the former employee will use any of this information for any improper purposes.

What We Are Doing?

The security and privacy of your information is of utmost importance to us. Immediately upon learning of the former employee's refusal to co-operate, we took steps to determine what information was on the hard drive and to notify appropriate authorities. We contacted law enforcement promptly and are pursuing appropriate action through law enforcement concerning the former employee and the information on the hard drive. We also are looking into changes to our controls and procedures to reduce the risk of similar events occurring in the future.

What You Can Do?

There are several steps you can take to protect your continued privacy and be sure that your information is not used improperly, many of which are good practices in any event.

First, in an abundance of caution, to help protect your identity, we are offering a complimentary two-year subscription to Experian's® credit monitoring and identity theft protection service, IdentityWorks. This product helps detect possible misuse of your personal information and provides you with superior identity theft detection and resolution support. To activate your membership and start monitoring your personal information please follow the steps below:

Activate Experian IdentityWorks Now in Three Easy Steps

1. **Ensure that you enroll by:** March 31, 2020 (Your code will not work after this date.)
2. **Visit the Experian IdentityWorks website to enroll:** https://www.experianidworks.com/credit
3. **Provide your activation code:** [ACTIVATION CODE]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877-716-5553** by **March 31, 2020**. Be prepared to provide engagement number **DB16594** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 24-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.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **877-716-5553**. 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 (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 this Identity Restoration support is available to you for one year 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. You will also find self-help tips and information about identity protection at this site.

Second, contact any financial institutions that you bank with and advise them of this situation, particularly if any of them use your social security number to identify or verify you. Check your accounts online or via telephone for any potential fraudulent activity. You should check your periodic statements from each such financial institution or credit card company promptly upon receiving them to be sure that no unauthorized transactions have occurred, and remain vigilant for incidents of fraud and identity theft.

Third, you should review any explanations of benefits, account statements, transaction confirmations that you receive by mail or email or any other similar communications you receive from institutions that you know. If you find any activity you do not recognize or that seems suspicious, you should contact the sender of that information immediately.

For More Information

For general information on protecting your privacy and preventing unauthorized use of your personal information, you may visit the U.S. Federal Trade Commission's Web site, http://ftc.gov or contact your state office of consumer affairs or attorney general.

* * *

We are committed to maintaining the security and privacy of the personal information you entrusted to us. We apologize for any inconvenience or concern this incident may cause. If we can be of any further assistance or answer any questions, please call 877-716-5553.

Sincerely,

Tyrina D. Blomer, Esq.
Vice President, Corporate Compliance and Privacy Officer
AmeriHealth Caritas Family of Companies