MEHAFFYWEBER
HOUSTON | BEAUMONT | SAN ANTONIO | AUSTIN

Adrian P. Senyszyn // *Shareholder*

Email AdrianSenyszyn@mehaffyweber.com

WWW.MEHAFFYWEBER.COM

North Dakota Attorney General
600 E. Boulevard Ave.
Dept. 125
Bismarck, ND 58505

Via Email: ndag@nd.gov

March 31, 2020

Re: Affordacare Urgent Care Clinics – Notice of Data Breach
MW 11380-0044

Dear Sir/Madam:

My office represents Affordacare Urgent Care Clinics ("Affordacare"). Affordacare's physical address is 2401 S Willis, Suite 103 Abilene, Texas 79605. Affordacare discovered that its servers suffered a Maze ransomware attack on or around February 1, 2020. Upon further investigation, Affordacare learned that hackers accessed its servers and removed some confidential information. Affordacare cannot determine the extent of confidential information removed. Twelve (12) North Dakota residents were potentially affected by the breach. The potentially affected information included the patient's name, address, telephone number, date of birth, age, date of visit, location of visit, reason for visit, insurance plan provider, insurance plan policy number, insurance group number, treatment codes and descriptions, and comments from the health care provider. Please note this incident *did not* affect electronic health records, labs, Social Security numbers, or any personal payment information. Additionally, the electronic health record system *was not* affected by this incident.

Since the attack, Affordacare safeguarded its systems in order to prevent further attacks and are no longer storing information on internal servers, thereby preventing data from being subject to attack in the future. Patients whose information was affected by this attack were notified on March 30, 2020, pursuant to state and federal requirements. A sample of an adult and minor notification letter is attached. The affected patients are being provided with twelve months of credit monitoring services, at no cost to the patients. The credit monitoring services include CyberScan Monitoring and a $1,000,000.00 insurance reimbursement policy. Additionally, Federal law enforcement authorities and local police departments were notified, and patients are being provided a copy of the police report upon request.

Sincerely,

Adrian P. Senyszyn
For the Firm

APS/jc
Enclosure-
Copy of Patient Notice Letters

AFFORDACARE
URGENT CARE CLINIC

To Enroll, Please Call:
(833) 570-0384
Or Visit:
https://ide.myidcare.com/affordacare
Enrollment Code: <<XXXXXXXX>>

C/O ID Experts
<<Return Address>>
<<City>>, <<State>> <<Zip>>

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

March 30, 2020

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

We are writing to notify you that a security breach occurred on or around February 1, 2020 involving a limited amount of your personal health care information.

What Happened

Affordacare Urgent Care Clinics ("Affordacare") discovered that its servers suffered a ransomware attack on or around February 1, 2020. Upon further investigation, Affordacare learned that hackers also accessed its servers and removed some confidential information as part of the attack. A limited amount of your confidential information may have been affected by the incident.

What Information Was Involved

Affordacare's servers contained limited confidential information about you. The potentially affected information included your name, address, telephone number, date of birth, age, date of visit, location of visit, reason for visit, insurance plan provider, insurance plan policy number, insurance group number, treatment codes and descriptions, and comments from the health care provider.

Please note this incident *did not* affect your electronic health records, labs, Social Security number or any personal payment information. The majority of your health care records are stored securely in an electronic health record system ("EHR"). The EHR *was not* affected by this incident.

What We Are Doing

Affordacare reported this incident to law enforcement and implemented additional safeguards to improve data security and prevent this kind of incident from occurring again. The affected servers were segregated from the network and the ransom *was not* paid. We are taking additional steps to protect patient-related data from theft or similar criminal activity in the future.

In addition, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (833) 570-0384 or going to https://ide.myidcare.com/affordacare using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is June 30, 2020.

We encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call (833) 570-0384 or go to https://ide.myidcare.com/affordacare for assistance or for any additional questions you may have.

Providing your urgent care needs is a privilege that we do not take for granted. Please know that we greatly value our relationship and wish you and your family continued good health.

Sincerely,

Affordacare Ownership and Management

MyIDCare™

Recommended Steps to Help Protect Your Information

1. **Website and Enrollment.** Go to https://ide.myidcare.com/affordacare and follow the instructions for enrollment using your Enrollment Code provided above.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at (833) 570-0384 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare 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 our ID Care team who will help you determine the cause of the suspicious items. In the unlikely 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.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: 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 www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center
Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

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

To Enroll, Please Call:
(833) 570-0384
Or Visit:
https://ide.myidcare.com/affordacare
Enrollment Code: <<XXXXXXXX>>

C/O ID Experts
<<Return Address>>
<<City>>, <<State>> <<Zip>>

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

March 30, 2020

Notice of Data Breach

Dear Parent or Guardian of <<First Name>> <<Last Name>>,

We are writing to notify you that a security breach occurred on or around February 1, 2020 involving a limited amount of your child's personal health care information.

What Happened

Affordacare Urgent Care Clinics ("Affordacare") discovered that its servers suffered a ransomware attack on or around February 1, 2020. Upon further investigation, Affordacare learned that hackers also accessed its servers and removed some confidential information as part of the attack. A limited amount of your child's confidential information may have been affected by the incident.

What Information Was Involved

Affordacare's servers contained limited confidential information about your child. The potentially affected information included your child's name, address, telephone number, date of birth, age, date of visit, location of visit, reason for visit, insurance plan provider, insurance plan policy number, insurance group number, treatment codes and descriptions, and comments from the health care provider.

Please note this incident *did not* affect your child's electronic health records, labs, Social Security number or any personal payment information. The majority of your child's health care records are stored securely in an electronic health record system ("EHR"). The EHR *was not* affected by this incident.

What We Are Doing

Affordacare reported this incident to law enforcement and implemented additional safeguards to improve data security and prevent this kind of incident from occurring again. The affected servers were segregated from the network and the ransom *was not* paid. We are taking additional steps to protect patient-related data from theft or similar criminal activity in the future.

In addition, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide your child with MyIDCare™. MyIDCare services include: 12 months of CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare will help you resolve issues if your child's identity is compromised.

What You Can Do

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (833) 570-0384 or going to https://ide.myidcare.com/affordacare using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is June 30, 2020.

We encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your child's personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call (833) 570-0384 or go to https://ide.myidcare.com/affordacare for assistance or for any additional questions you may have.

Providing your child's urgent care needs is a privilege that we do not take for granted. Please know that we greatly value our relationship and wish you and your family continued good health.

Sincerely,

Affordacare Ownership and Management

MyIDCare™

Recommended Steps to Help Protect Your Information

1. **Website and Enrollment.** Go to https://ide.myidcare.com/affordacare and follow the instructions for enrollment using your Enrollment Code provided above.

2. Activate the CyberScan monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at (833) 570-0384 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your child's credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare 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 our ID Care team who will help you determine the cause of the suspicious items. In the unlikely 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.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your child's credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your child's existing accounts. For that reason, placing a fraud alert can protect your child, but also may delay you when you seek to obtain credit on their behalf. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your child's personal identifying information will not be able to use that information to open new accounts or borrow money in thier name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, your child will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: 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 www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center
Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

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