Richard Reiter
914.872.7728 (direct)
Richard.Reiter@wilsonelser.com

September 9, 2021

Via Online Submission

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Data Security Incident

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents HealthReach Community Health Centers, located at 10 Water Street, Suite 305, Waterville, ME 04901, with respect to a data security incident described in more detail below. HealthReach Community Health Centers takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Description of the Incident.

On or about May 7, 2021, HealthReach Community Health Centers was notified that hard drives containing information belonging to HealthReach Community Health Centers' patients and employees were improperly disposed of by an employee at a third-party data storage facility (the "Incident"). HealthReach Community Health Centers has since worked diligently to determine exactly what happened and what information was involved as a result of this Incident.

Based on the results of an investigation conducted by third-party forensic vendors, HealthReach Community Health Centers determined that the following elements of personal information may potentially be accessed and/or acquired by an unauthorized individual: names, addresses, dates of birth, social security numbers, medical record number, medical insurance information, lab results, treatment records and financial account information. The exact elements of personal information that may have be exposed as a result of this incident varies per individual.

As of this writing, HealthReach Community Health Centers has not received any reports of fraud or identity theft related to this matter.

2. Number of Maine residents affected.

HealthReach Community Health Centers discovered that the Incident may have resulted in the unauthorized exposure of information pertaining to one hundred thousand, three hundred and ninety-five (101,395) Maine residents. Notification letters to these individuals will be mailed on September 9, 2021, via First Class Mail. Sample copies of the notification letters are attached as **Exhibit A**.

3. Steps taken.

Upon discovery of the Incident, HealthReach Community Health Centers worked with cybersecurity counsel to investigate how the Incident occurred and what information was potentially compromised. HealthReach Community Health Centers is committed to ensuring the security of all information in its control, and is taking steps to prevent a similar event from occurring in the future, including ensuring our data storage vendors re-train employees and comply with the required safeguards as to the disposal of sensitive information. Additionally, all notified Maine residents whose social security number and/or financial account information were potentially compromised were offered complimentary identity theft and credit monitoring services for twelve (12) months.

4. Contact information.

HealthReach Community Health Centers remains dedicated to protecting the sensitive information within its control. If you have any questions or need additional information, please do not hesitate to contact me at Richard.Reiter@wilsonelser.com or (914) 872-7728.

Very truly yours,

WILSON ELSER MOSKOWITZ EDELMAN AND DICKER LLP

Richard Reiter

Richard Reiter

EXHIBIT A

HealthReach
Community Health Centers
P.O Box 989728
West Sacramento, CA 95798-9728

10 Water Street, Suite 305
Waterville, ME 04901

To Enroll, Please Visit:
https://response.idx.us/hrchc

Or Call:
1-833-992-4004

Enrollment Code:
<<XXXXXXXX>>

Via First-Class Mail

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

September 7, 2021

Notice of Data Incident

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

HealthReach Community Health Centers recently experienced a data security incident which may have affected your personal information. We take the protection and proper use of your information seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains additional information about the incident, our response to this incident, and steps you can take to protect yourself.

What Happened

On or about May 7, 2021, HealthReach Community Health Centers was notified that hard drives containing information belonging to HealthReach Community Health Centers' patients and employees were improperly disposed of by an employee at a third-party data storage facility. We have since worked diligently to determine exactly what happened and what information was involved as a result of this incident.

What Information Was Involved

The elements of your personal information that were exposed may have included, and potentially were not limited to: your name, address, date of birth, social security number, medical record number, medical insurance information, lab results and treatment records. Please note that there is no evidence at this time that any of your personal information has been misused as a result of this incident.

What We Are Doing

We are working with cybersecurity counsel to determine the actions to take in response to the incident. Together, we continue to investigate and closely monitor the situation. Further, we are taking steps to prevent a similar event from occurring again in the future, including ensuring our data storage vendors re-train employees and comply with the required safeguards as to the disposal of sensitive information.

Out of an abundance of caution, we have arranged for you to enroll in a complementary, identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: twelve (12) months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

To enroll in the complimentary credit monitoring service that we are offering you, please go to https://response.idx.us/hrchc and using Enrollment Code <<XXXXXXXX>>, follow the steps to receive the credit monitoring service

online within minutes. If you do not have access to the Internet and wish to enroll, please call IDX's toll-free hotline at 1-833-992-4004.

You can sign up for the online or offline credit monitoring service anytime between now and December 7, 2021. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, the daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

We encourage you to remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information.

For More Information

Please know that the protection of your personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call 1-833-992-4004, Monday – Friday, 9 am – 9 am Eastern Time.

Sincerely,

HealthReach Community Health Centers

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft **For residents of *Massachusetts*:** It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion(https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

HealthReach
Community Health Centers
P.O Box 989728
West Sacramento, CA 95798-9728

10 Water Street, Suite 305
Waterville, ME 04901

Via First-Class Mail

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

September 7, 2021

Notice of Data Incident

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

HealthReach Community Health Centers recently experienced a data security incident which may have affected your personal information. We take the protection and proper use of your information seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains additional information about the incident, our response to this incident, and steps you can take to protect yourself.

What Happened

On or about May 7, 2021, HealthReach Community Health Centers was notified that hard drives containing information belonging to HealthReach Community Health Centers' patients were improperly disposed of by an employee at a third-party data storage facility. We have since worked diligently to determine exactly what happened and what information was involved as a result of this incident.

What Information Was Involved

The elements of your personal information that were exposed may have included, and potentially were not limited to: your name, address, date of birth, social security number, medical record number, medical insurance information, lab results and treatment records. Please note that there is no evidence at this time that any of your personal information has been misused as a result of this incident.

What We Are Doing

We are working with cybersecurity counsel to determine the actions to take in response to the incident. Together, we continue to investigate and closely monitor the situation. Further, we are taking steps to prevent a similar event from occurring again in the future, including ensuring our data storage vendors comply with the required safeguards as to the disposal of sensitive information.

What You Can Do

At this time, we are not aware of anyone experiencing fraud as a result of this incident. We encourage you to remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. Additionally, we recommend that you review the following page, which contains important additional

information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes.

For More Information

Please know that the protection of your personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call 1-833-992-4004, Monday – Friday, 9 am – 9 pm Eastern Time.

Sincerely,

HealthReach Community Health Centers

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft **For residents of *Massachusetts*:** It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion(https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

HealthReach
Community Health Centers
P.O Box 989728
West Sacramento, CA 95798-9728

10 Water Street, Suite 305
Waterville, ME 04901

To Enroll, Please Visit:
https://response.idx.us/hrchc

Or Call:
1-833-992-4004

Enrollment Code:
<<XXXXXXXX>>

Via First-Class Mail

TO THE PARENT OR GUARDIAN OF
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

September 7, 2021

Notice of Data Incident

To the Parent or Guardian of <<First Name>><<Last Name>>:

HealthReach Community Health Centers recently experienced a data security incident which may have affected your child's personal information. We take the protection and proper use of your child's information seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains additional information about the incident, our response to this incident, and steps you can take to protect your child.

What Happened

On or about May 7, 2021, HealthReach Community Health Centers was notified that hard drives containing information belonging to HealthReach Community Health Centers' patients were improperly disposed of by an employee at a third-party data storage facility. We have since worked diligently to determine exactly what happened and what information was involved as a result of this incident.

What Information Was Involved

The elements of your child's personal information that were exposed may have included, and potentially were not limited to: your child's name, address, date of birth, social security number, medical record number, medical insurance information, lab results and treatment records. Please note that there is no evidence at this time that any of your child's personal information has been misused as a result of this incident.

What We Are Doing

We are working with cybersecurity counsel to determine the actions to take in response to the incident. Together, we continue to investigate and closely monitor the situation. Further, we are taking steps to prevent a similar event from occurring again in the future, including ensuring our data storage vendors re-train employees and comply with the required safeguards as to the disposal of sensitive information.

Out of an abundance of caution, we have arranged for you to enroll in a complementary, identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: twelve (12) months CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your child's identity is compromised.

What You Can Do

To enroll in the complimentary monitoring service that we are offering your child, please go to https://response.idx.us/hrchc and using Enrollment Code <<XXXXXXXX>>, follow the steps to receive the credit monitoring service

within minutes. If you do not have access to the Internet and wish to enroll, please call IDX's toll-free hotline at 1-833-992-4004.

You can sign up for service anytime between now and December 7, 2021. Due to privacy laws, we cannot register you directly.

Once enrolled, you will be able to obtain twelve (12) months of unlimited Cyberscan dark web monitoring. CyberScan monitoring which will monitor criminal websites, chat rooms, and bulletin boards for illegal selling or trading of your child's personal information. The service also includes access to an identity restoration program that provides assistance in the event that your child's identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

We encourage you to remain vigilant and immediately report any suspicious activity or suspected misuse of your child's personal information.

For More Information

Please know that the protection of your child's personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call 1-833-992-4004, Monday – Friday, 9 am – 9 pm Eastern Time.

Sincerely,

HealthReach Community Health Centers

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft **For residents of *Massachusetts*:** It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion(https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

HealthReach
Community Health Centers
P.O Box 989728
West Sacramento, CA 95798-9728

10 Water Street, Suite 305
Waterville, ME 04901

Via First-Class Mail

TO THE PARENT OR GUARDIAN OF
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

September 7, 2021

Notice of Data Incident

To the Parent or Guardian of <<First Name>> <<Last Name>>:

HealthReach Community Health Centers recently experienced a data security incident which may have affected your child's personal information. We take the protection and proper use of your child's information seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains additional information about the incident, our response to this incident, and steps you can take to protect your child.

What Happened

On or about May 7, 2021, HealthReach Community Health Centers was notified that hard drives containing information belonging to HealthReach Community Health Centers' patients were improperly disposed of by an employee at a third-party data storage facility. We have since worked diligently to determine exactly what happened and what information was involved as a result of this incident.

What Information Was Involved

The elements of your child's personal information that were exposed may have included, and potentially were not limited to: your child's name, address, date of birth, medical record number, medical insurance information, lab results and treatment records. Please note that there is no evidence at this time that any of your child's personal information has been misused as a result of this incident.

What We Are Doing

We are working with cybersecurity counsel to determine the actions to take in response to the incident. Together, we continue to investigate and closely monitor the situation. Further, we are taking steps to prevent a similar event from occurring again in the future, including ensuring our data storage vendors re-train employees and comply with the required safeguards as to the disposal of sensitive information.

What You Can Do

At this time, we are not aware of anyone experiencing fraud as a result of this incident. We encourage you to remain vigilant and immediately report any suspicious activity or suspected misuse of your child's personal information. Additionally, we recommend that you review the following page, which contains important additional information about steps you can take to safeguard your child's personal information, such as the implementation of fraud alerts and security freezes.

For More Information

Please know that the protection of your child's personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call 1-833-992-4004, Monday – Friday, Monday – Friday, 9 am – 9 pm Eastern Time.

Sincerely,

HealthReach Community Health Centers

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft **For residents of *Massachusetts*:** It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion(https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

HealthReach
Community Health Centers
P.O Box 989728
West Sacramento, CA 95798-9728

10 Water Street, Suite 305
Waterville, ME 04901

Via First-Class Mail

TO THE ESTATE OF
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

September 7, 2021

Notice of Data Incident

To the Representative of the Estate of <<First Name>> <<Last Name>>:

HealthReach Community Health Centers recently experienced a data security incident which may have affected the decedent's personal information. We take the protection and proper use of the information in our control seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains additional information about the incident, our response to this incident, and resources we are making available to you.

What Happened

On or about May 7, 2021, HealthReach Community Health Centers was notified that hard drives containing information belonging to HealthReach Community Health Centers' patients were improperly disposed of by an employee at a third-party data storage facility. We have since worked diligently to determine exactly what happened and what information was involved as a result of this incident.

What Information Was Involved

The elements of the decedent's personal information that were exposed may have included, and potentially were not limited to: the decedent's name, address, date of birth, social security number, medical record number, medical insurance information, lab results and treatment records. Please note that there is no evidence at this time that any of the decedent's personal information has been misused as a result of this incident.

What We Are Doing

We are working with cybersecurity counsel to determine the actions to take in response to the incident. Together, we continue to investigate and closely monitor the situation. Further, we are taking steps to prevent a similar event from occurring again in the future, including ensuring our data storage vendors re-train employees and comply with the required safeguards as to the disposal of sensitive information.

What You Can Do

At this time, we are not aware of anyone experiencing fraud as a result of this incident. We encourage you to remain vigilant and immediately report any suspicious activity or suspected misuse of the decedent's personal information. Additionally, we recommend that you review the following page, which contains important additional information about steps you can take to safeguard the decedent's personal information, such as the implementation of fraud alerts and security freezes.

For More Information

Please know that the protection of the decedent's personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call 1-833-992-4004, Monday – Friday, 9 am – 9 pm Eastern Time.

Sincerely,

HealthReach Community Health Centers

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft **For residents of *Massachusetts*:** It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion(https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

HealthReach
Community Health Centers
P.O Box 989728
West Sacramento, CA 95798-9728

10 Water Street, Suite 305
Waterville, ME 04901

To Enroll, Please Visit:
https://response.idx.us/hrchc

Or Call:
1-833-992-4004

Enrollment Code:
<<XXXXXXXX>>

Via First-Class Mail

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

September 7, 2021

Notice of Data Incident

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

HealthReach Community Health Centers recently experienced a data security incident which may have affected your personal information. We take the protection and proper use of your information seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains additional information about the incident, our response to this incident, and steps you can take to protect yourself.

What Happened

On or about May 7, 2021, HealthReach Community Health Centers was notified that hard drives containing information belonging to certain HealthReach Community Health Centers' employees were improperly disposed of by an employee at a third-party data storage facility. We have since worked diligently to determine exactly what happened and what information was involved as a result of this incident.

What Information Was Involved

The elements of your personal information that were exposed may have included, and potentially were not limited to: your name, address, date of birth, social security number and financial account information. Please note that there is no evidence at this time that any of your personal information has been misused as a result of this incident.

What We Are Doing

We are working with cybersecurity counsel to determine the actions to take in response to the incident. Together, we continue to investigate and closely monitor the situation. Further, we are taking steps to prevent a similar event from occurring again in the future, including ensuring our data storage vendors re-train employees and comply with the required safeguards as to the disposal of sensitive information.

Out of an abundance of caution, we have arranged for you to enroll in a complementary, identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: twelve (12) months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

To enroll in the complimentary credit monitoring service that we are offering you, please go to https://response.idx.us/hrchc and using Enrollment Code <<XXXXXXXX>>, follow the steps to receive the credit monitoring service

online within minutes. If you do not have access to the Internet and wish to enroll, please call IDX's toll-free hotline at 1-833-992-4004.

You can sign up for the online or offline credit monitoring service anytime between now and December 7, 2021. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, the daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

We encourage you to remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information.

For More Information

Please know that the protection of your personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call 1-833-992-4004, Monday – Friday, 9 am – 9 pm Eastern Time.

Sincerely,

HealthReach Community Health Centers

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft **For residents of *Massachusetts*:** It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion(https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

HealthReach
Community Health Centers
P.O Box 989728
West Sacramento, CA 95798-9728

10 Water Street, Suite 305
Waterville, ME 04901

To Enroll, Please Visit:
https://response.idx.us/hrchc

Or Call:
1-833-992-4004

Enrollment Code:
<<XXXXXXXX>>

Via First-Class Mail

TO THE ESTATE OF
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

September 7, 2021

Notice of Data Incident

To the Representative of the Estate of

HealthReach Community Health Centers recently experienced a data security incident which may have affected the decedent's personal information. We take the protection and proper use of the information in our control seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains additional information about the incident, our response to this incident, and resources we are making available to you.

What Happened

On or about May 7, 2021, HealthReach Community Health Centers was notified that hard drives containing information belonging to HealthReach Community Health Centers' patients were improperly disposed of by an employee at a third-party data storage facility. We have since worked diligently to determine exactly what happened and what information was involved as a result of this incident.

What Information Was Involved

The elements of the decedent's personal information that were exposed may have included, and potentially were not limited to: the decedent's name, address, date of birth, social security number, medical record number, medical insurance information, lab results and treatment records. Please note that there is no evidence at this time that any of the decedent's personal information has been misused as a result of this incident.

What We Are Doing

We are working with cybersecurity counsel to determine the actions to take in response to the incident. Together, we continue to investigate and closely monitor the situation. Further, we are taking steps to prevent a similar event from occurring again in the future, including ensuring our data storage vendors re-train employees and comply with the required safeguards as to the disposal of sensitive information.

Out of an abundance of caution, we have arranged for you to enroll in a complementary, identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: twelve (12) months of CyberScan monitoring, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if the decedent's identity is compromised.

What You Can Do

To enroll in the complimentary identity theft monitoring service that we are offering the decedent's estate, please go to https://response.idx.us/hrchc and using Enrollment Code <<XXXXXXXX>>, follow the steps to receive the

identity theft monitoring service online within minutes. If you do not have access to the Internet and wish to enroll, please call IDX's toll-free hotline at 1-833-992-4004.

You can sign up for the online or offline identity theft monitoring service anytime between now and December 7, 2021. Due to privacy laws, we cannot register the decedent directly.

Once enrolled, you will obtain twelve (12) months of unlimited of CyberScan monitoring, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if the decedent's identity is compromised. CyberScan monitoring which will monitor criminal websites, chat rooms, and bulletin boards for illegal selling or trading of the decedent's personal information. The service also includes access to an identity restoration program that provides assistance in the event that the decedent's identity is compromised.
We encourage you to remain vigilant and immediately report any suspicious activity or suspected misuse of the decedent's personal information.

For More Information

Please know that the protection of the decedent's personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call 1-833-992-4004, Monday – Friday, 9 am – 9 pm Eastern Time.

Sincerely,

HealthReach Community Health Centers

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft **For residents of *Massachusetts*:** It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion(https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

HealthReach
Community Health Centers
P.O Box 989728
West Sacramento, CA 95798-9728

10 Water Street, Suite 305
Waterville, ME 04901

To Enroll, Please Visit:
https://response.idx.us/hrchc

Or Call:
1-833-992-4004

Enrollment Code:
<<XXXXXXXX>>

Via First-Class Mail

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

September 7, 2021

Notice of Data Incident

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

HealthReach Community Health Centers recently experienced a data security incident which may have affected your personal information. We take the protection and proper use of your information seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains additional information about the incident, our response to this incident, and steps you can take to protect yourself.

What Happened

On or about May 7, 2021, HealthReach Community Health Centers was notified that hard drives containing information belonging to HealthReach Community Health Centers' patients and employees were improperly disposed of by an employee at a third-party data storage facility. We have since worked diligently to determine exactly what happened and what information was involved as a result of this incident.

What Information Was Involved

The elements of your personal information that were exposed may have included, and potentially were not limited to: your name, address, date of birth, social security number, medical record number, medical insurance information, lab results and treatment records. Please note that there is no evidence at this time that any of your personal information has been misused as a result of this incident.

What We Are Doing

We are working with cybersecurity counsel to determine the actions to take in response to the incident. Together, we continue to investigate and closely monitor the situation. Further, we are taking steps to prevent a similar event from occurring again in the future, including ensuring our data storage vendors re-train employees and comply with the required safeguards as to the disposal of sensitive information.

Out of an abundance of caution, we have arranged for you to enroll in a complementary, identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: twenty-four (24) months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

To enroll in the complimentary credit monitoring service that we are offering you, please go to https://response.idx.us/hrchc and using Enrollment Code <<XXXXXXXX>>, follow the steps to receive the credit monitoring service

online within minutes. If you do not have access to the Internet and wish to enroll, please call IDX's toll-free hotline at 1-833-992-4004.

You can sign up for the online or offline credit monitoring service anytime between now and December 7, 2021. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, the daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

We encourage you to remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information.

For More Information

Please know that the protection of your personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call 1-833-992-4004, Monday – Friday, 9 am – 9 pm Eastern Time.

Sincerely,

HealthReach Community Health Centers

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft **For residents of *Massachusetts*:** It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion(https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

HealthReach
Community Health Centers
P.O Box 989728
West Sacramento, CA 95798-9728

10 Water Street, Suite 305
Waterville, ME 04901

To Enroll, Please Visit:
https://response.idx.us/hrchc

Or Call:
1-833-992-4004

Enrollment Code:
<<XXXXXXXX>>

Via First-Class Mail

TO THE PARENT OR GUARDIAN OF
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

September 7, 2021

Notice of Data Incident

To the Parent or Guardian of <<First Name>> <<Last Name>>:

HealthReach Community Health Centers recently experienced a data security incident which may have affected your child's personal information. We take the protection and proper use of your child's information seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains additional information about the incident, our response to this incident, and steps you can take to protect your child.

What Happened

On or about May 7, 2021, HealthReach Community Health Centers was notified that hard drives containing information belonging to HealthReach Community Health Centers' patients were improperly disposed of by an employee at a third-party data storage facility. We have since worked diligently to determine exactly what happened and what information was involved as a result of this incident.

What Information Was Involved

The elements of your child's personal information that were exposed may have included, and potentially were not limited to: your child's name, address, date of birth, social security number, medical record number, medical insurance information, lab results and treatment records. Please note that there is no evidence at this time that any of your child's personal information has been misused as a result of this incident.

What We Are Doing

We are working with cybersecurity counsel to determine the actions to take in response to the incident. Together, we continue to investigate and closely monitor the situation. Further, we are taking steps to prevent a similar event from occurring again in the future, including ensuring our data storage vendors re-train employees and comply with the required safeguards as to the disposal of sensitive information.

Out of an abundance of caution, we have arranged for you to enroll in a complementary, identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: twenty-four (24) months of CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your child's identity is compromised.

What You Can Do

To enroll in the complimentary monitoring service that we are offering your child, please go to https://response.idx.us/hrchc and using Enrollment Code <<XXXXXXXX>>, follow the steps to receive the credit monitoring service online

within minutes. If you do not have access to the Internet and wish to enroll, please call IDX's toll-free hotline at 1-833-992-4004.

You can sign up for the service anytime between now and December 7, 2021. Due to privacy laws, we cannot register you directly.

Once enrolled, you will be able to obtain twenty-four (24) months of unlimited Cyberscan dark web monitoring. CyberScan monitoring which will monitor criminal websites, chat rooms, and bulletin boards for illegal selling or trading of your personal information. The service also includes access to an identity restoration program that provides assistance in the event that your child's identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

We encourage you to remain vigilant and immediately report any suspicious activity or suspected misuse of your child's personal information.

For More Information

Please know that the protection of your child's personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call 1-833-992-4004, Monday – Friday, 9 am – 9 pm Eastern Time.

Sincerely,

HealthReach Community Health Centers

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft **For residents of *Massachusetts*:** It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion(https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

HealthReach
Community Health Centers
P.O Box 989728
West Sacramento, CA 95798-9728

10 Water Street, Suite 305
Waterville, ME 04901

To Enroll, Please Visit:
https://response.idx.us/hrchc

Or Call:
1-833-992-4004

Enrollment Code:
<<XXXXXXXX>>

Via First-Class Mail

TO THE ESTATE OF
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

September 7, 2021

Notice of Data Incident

To the Representative of the Estate of <<First Name>> <<Last Name>>:

HealthReach Community Health Centers recently experienced a data security incident which may have affected the decedent's personal information. We take the protection and proper use of the information in our control seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains additional information about the incident, our response to this incident, and resources we are making available to you.

What Happened

On or about May 7, 2021, HealthReach Community Health Centers was notified that hard drives containing information belonging to HealthReach Community Health Centers' patients were improperly disposed of by an employee at a third-party data storage facility. We have since worked diligently to determine exactly what happened and what information was involved as a result of this incident.

What Information Was Involved

The elements of the decedent's personal information that were exposed may have included, and potentially were not limited to: the decedent's name, address, date of birth, social security number, medical record number, medical insurance information, lab results and treatment records. Please note that there is no evidence at this time that any of the decedent's personal information has been misused as a result of this incident.

What We Are Doing

We are working with cybersecurity counsel to determine the actions to take in response to the incident. Together, we continue to investigate and closely monitor the situation. Further, we are taking steps to prevent a similar event from occurring again in the future, including ensuring our data storage vendors re-train employees and comply with the required safeguards as to the disposal of sensitive information.

Out of an abundance of caution, we have arranged for you to enroll in a complementary, identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: twenty-four (24) months of CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if the decedent's identity is compromised.

What You Can Do

To enroll in the complimentary identity theft monitoring service that we are offering the decedent's estate, please go to https://response.idx.us/hrchc and using Enrollment Code <<XXXXXXXX>>, follow the steps to receive

monitoring service online within minutes. If you do not have access to the Internet and wish to enroll, please call IDX's toll-free hotline at 1-833-992-4004.

You can sign up for the online or offline identity theft monitoring service anytime between now and December 7, 2021. Due to privacy laws, we cannot register the decedent directly.

Once enrolled, you will be able to obtain twenty-four (24) months of of CyberScan monitoring, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if the decedent's identity is compromised. CyberScan monitoring which will monitor criminal websites, chat rooms, and bulletin boards for illegal selling or trading of the decedent's personal information.The service also includes access to an identity restoration program that provides assistance in the event that the decedent's identity is compromised.

We encourage you to remain vigilant and immediately report any suspicious activity or suspected misuse of the decedent's personal information.

For More Information

Please know that the protection of the decedent's personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call 1-833-992-4004, Monday – Friday, 9 am – 9 pm Eastern Time.

Sincerely,

HealthReach Community Health Centers

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft **For residents of *Massachusetts*:** It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion(https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

HealthReach
Community Health Centers
P.O Box 989728
West Sacramento, CA 95798-9728

10 Water Street, Suite 305
Waterville, ME 04901

To Enroll, Please Visit:
https://response.idx.us/hrchc

Or Call:
1-833-992-4004

Enrollment Code:
<<XXXXXXXX>>

Via First-Class Mail

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

September 7, 2021

Notice of Data Incident

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

HealthReach Community Health Centers recently experienced a data security incident which may have affected your personal information. We take the protection and proper use of your information seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains additional information about the incident, our response to this incident, and steps you can take to protect yourself.

What Happened

On or about May 7, 2021, HealthReach Community Health Centers was notified that hard drives containing information belonging to certain HealthReach Community Health Centers' employees were improperly disposed of by an employee at a third-party data storage facility. We have since worked diligently to determine exactly what happened and what information was involved as a result of this incident.

What Information Was Involved

The elements of your personal information that were exposed may have included, and potentially were not limited to: your name, address, date of birth, social security number and financial account information. Please note that there is no evidence at this time that any of your personal information has been misused as a result of this incident.

What We Are Doing

We are working with cybersecurity counsel to determine the actions to take in response to the incident. Together, we continue to investigate and closely monitor the situation. Further, we are taking steps to prevent a similar event from occurring again in the future, including ensuring our data storage vendors re-train employees and comply with the required safeguards as to the disposal of sensitive information.

Out of an abundance of caution, we have arranged for you to enroll in a complementary, identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: twenty-four (24) months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

To enroll in the complimentary credit monitoring service that we are offering you, please go to https://response.idx.us/hrchc and using Enrollment Code <<XXXXXXXX>>, follow the steps to receive the credit monitoring service

online within minutes. If you do not have access to the Internet and wish to enroll, please call IDX's toll-free hotline at 1-833-992-4004.

You can sign up for the online or offline credit monitoring service anytime between now and December 7, 2021. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, the daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

We encourage you to remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information.

For More Information

Please know that the protection of your personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call 1-833-992-4004, Monday – Friday, 9 am – 9 pm Eastern Time.

Sincerely,

HealthReach Community Health Centers

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft **For residents of *Massachusetts*:** It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion(https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.