DEMARCO LAW, PLLC

ATTORNEYS AND COUNSELORS AT LAW

**Joseph V. DeMarco**
Telephone:
212.922.9499
jvd@demarcolaw.com

January 31, 2025

VIA FIRST CLASS MAIL
Office of the Attorney General
150 South Main Street
Providence, RI 02903

***RE:* SECURITY BREACH NOTIFICATION**

To Whom It May Concern:

We are counsel to the Community Health Center, Inc. (CHC), a federally qualified health center headquartered in Middletown, Connecticut.

On January 2, 2025, staff became aware of unusual activity within CHC IT systems. That same day, a leading independent forensics firm was retained to conduct a thorough investigation and help secure the environment. The investigation concluded that a sophisticated criminal actor had accessed the IT environment and successfully acquired CHC data, likely including the electronic health record database, and moved a copy of it to a location under the criminal actor's control. The criminal actor did not delete or encrypt any CHC data and the incident did not significantly impact clinical or business operations. The criminal actor's access was revoked within hours of discovering it. As a result of the incident, CHC has implemented additional technical safeguards.

The personal and protected health information involved falls into one of two classes: (1) regular CHC patients and (2) individuals who received a COVID test or vaccine at a mass testing or vaccine site during the pandemic.

The incident impacted 1,060,936 total individuals, including 2,042 Rhode Island residents. CHC sent written notifications to 7,248 impacted Rhode Island residents on January 30, 2025, with an offer of 24 months of complimentary identity theft protection services. A template letter is enclosed herein. For 90 individuals for whom we do not have contact information, CHC is providing substitute notice.

For regular CHC patients, the information includes all information in the CHC medical record system (including Social Security Number (SSN) for many. All CHC patients are receiving an offer of 24 months identity theft prevention services (ITPS).

Community Health Center, Inc.
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/CommunityHealthCenter

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

January 30, 2025

**Notice of Data Breach**

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

You are receiving this letter because you are a current or former patient of Community Health Center, Inc. ("CHC"). We are writing to inform you of a data security incident that may have exposed your personal information. We take your privacy seriously, so we want to share details of the incident and how you can protect your personal information.

**What Happened**

On January 2, 2025, we noticed unusual activity in our computer systems. That same day, we brought in experts to investigate and reinforce the security of our systems. They found that a skilled criminal hacker got into our system and took some data, which might include your personal information. Fortunately, the criminal hacker did not delete or lock any of our data, and the criminal's activity did not affect our daily operations. We believe we stopped the criminal hacker's access within hours, and that there is no current threat to our systems.

**What Information Was Involved**

The personal information that may have been accessed or taken includes information in your health record at CHC. This might include your name, date of birth, address, phone number, email, diagnoses, treatment details, test results, Social Security number, and health insurance information.

**What We Are Doing**

We've strengthened our security and added special software to watch for suspicious activity. We are also working to make sure your information stays safe in the future.

So far, there is no sign that your information has been misused. To help protect you, we're offering free identity theft protection through IDX. IDX is a company that we've hired to help protect you and answer your questions. These services include:

- 24 months of credit and CyberScan monitoring
- A $1,000,000 insurance reimbursement policy
- Help recovering your identity if it is stolen

If you need help, IDX will work with you to fix any issues with your identity.

IDX
A ZEROFOX COMPANY

**Recommended Steps to help Protect your Information**

1. **Website and Enrollment.** Go to https://response.idx.us/CommunityHealthCenter and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

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

3. **Telephone.** Contact IDX at 1-877-229-9277 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

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

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

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

**Credit Bureaus**

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

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

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

6. **Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place

Community Health Center, Inc.
P.O. Box 989728
West Sacramento, CA 95798-9728

To the Parent or Guardian of
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/CommunityHealthCenter

January 30, 2025

**Notice of Data Breach**

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

You are receiving this letter because your child is a current or former patient of Community Health Center, Inc. ("CHC"). We are writing to inform you of a data security incident that may have exposed your child's personal information. We take your child's privacy seriously, so we want to share details of the incident and how you can protect your child's personal information.

**What Happened**

On January 2, 2025, we noticed unusual activity in our computer systems. That same day, we brought in experts to investigate and reinforce the security of our systems. They found that a skilled criminal hacker got into our system and took some data, which might include your child's personal information. Fortunately, the criminal hacker did not delete or lock any of our data, and the criminal's activity did not affect our daily operations. We believe we stopped the criminal hacker's access within hours, and that there is no current threat to our systems.

**What Information Was Involved**

The personal information that may have been accessed or taken includes information in your child's health record at CHC, including name, date of birth, address, phone, email, guarantor information, diagnoses, progress notes, medications, treatment information, test results, records received from other providers, Social Security Number, and health insurance information.

**What We Are Doing**

We've strengthened our security and added special software to watch for suspicious activity. We are also working to make sure your information stays safe in the future.

So far, there is no sign that your child's information has been misused. To help protect you, we're offering free identity theft protection through IDX. IDX is a company that we've hired to help protect you and answer your questions. These services include:

- 24 months of CyberScan monitoring
- A $1,000,000 insurance reimbursement policy
- Help recovering your identity if it is stolen

IDX
A ZEROFOX COMPANY

**Recommended Steps to help Protect your Information**

**1. Website and Enrollment.** Go to https://response.idx.us/CommunityHealthCenter and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

**2. Telephone.** Contact IDX at 1-877-229-9277 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

**3. Watch for Suspicious Activity**. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

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

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

**4. Security Freeze.** You may place a free credit freeze for children under age 16. By placing a security freeze, someone who fraudulently acquires your child's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the three national credit reporting bureaus listed below to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your child's credit files.

**Credit Bureaus**

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

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

**California Residents:** Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

**Connecticut Residents:** The Attorney General may be contacted at: 165 Capitol Avenue, Hartford, CT 06106; 1-860-808-5318; https://portal.ct.gov/AG.

**District of Columbia:** Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

**Iowa Residents:** You should report any suspected identity theft to law enforcement or to the Iowa Attorney General, Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Community Health Center, Inc.
P.O. Box 989728
West Sacramento, CA 95798-9728

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

January 30, 2025

**Notice of Data Breach**

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

You are receiving this letter because you received a COVID test and/or COVID vaccination at a clinic operated by Community Health Center, Inc. ("CHC"). We are writing to inform you of a data security incident that may have exposed your personal information. We take your privacy seriously, so we want to share details of the incident and how you can protect your personal information.

**What Happened**

On January 2, 2025, we noticed unusual activity in our computer systems. That same day, we brought in experts to investigate and reinforce the security of our systems. They found that a skilled criminal hacker got into our system and took some data, which might include your personal information. Fortunately, the criminal hacker did not delete or lock any of our data, and the criminal's activity did not affect our daily operations. We believe we stopped the criminal hacker's access within hours, and that there is no current threat to our systems.

**What Information Was Involved**

If you received COVID testing or vaccine services from CHC, the personal information that may have been impacted includes your name, date of birth, phone number, email, address, gender, race, and ethnicity. For testing only patients, the date of test and result information was also involved. For vaccine patients, health insurance information, guarantor name and vaccine type, dose and date administered may also have been involved.

**What We Are Doing**

We've strengthened our security and added special software to watch for suspicious activity. We are also working to make sure your information stays safe in the future.

**What You Can Do**

We have partnered with IDX to answer questions and provide valuable information about the incident. We encourage you to contact IDX with any questions by calling 1-877-229-9277. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time.

At this time, there is no evidence that your information has been misused. The team at IDX knows all about the situation and can answer any questions or concerns you have about keeping your personal information safe.

IDX
A ZEROFOX COMPANY

**Recommended Steps to help Protect your Information**

**1. Telephone.** Contact IDX at 1-877-229-9277 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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

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

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

**Credit Bureaus**

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

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

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

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

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

**California Residents:** Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Community Health Center, Inc.
P.O. Box 989728
West Sacramento, CA 95798-9728

To the Parent or Guardian of
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

January 30, 2025

**Notice of Data Breach**

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

You are receiving this letter because your child received a COVID test and/or COVID vaccination at a clinic operated by Community Health Center, Inc. ("CHC"). We are writing to inform you of a data security incident that may have exposed your child's personal information. We take your child's privacy seriously, so we want to share details of the incident and how you can protect your child's personal information.

**What Happened**

On January 2, 2025, we noticed unusual activity in our computer systems. That same day, we brought in experts to investigate and reinforce the security of our systems. They found that a skilled criminal hacker got into our system and took some data, which might include your child's personal information. Fortunately, the criminal hacker did not delete or lock any of our data, and the criminal's activity did not affect our daily operations. We believe we stopped the criminal hacker's access within hours, and that there is no current threat to our systems.

**What Information Was Involved**

If your child received COVID testing or vaccine services from CHC, the personal information that may have been impacted includes your child's name, date of birth, phone number, email, address, gender, race, and ethnicity. For testing only patients, the date of test and result information was also involved. For vaccine patients, health insurance information, guarantor name and vaccine type, dose and date administered may also have been involved.

**What We Are Doing**

We've strengthened our security and added special software to watch for suspicious activity. We are also working to make sure your information stays safe in the future.

**What You Can Do**

We have partnered with IDX to answer questions and provide valuable information about the incident. We encourage you to contact IDX with any questions by calling 1-877-229-9277. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time.

At this time, there is no evidence that your child's information has been misused. The team at IDX knows all about the situation and can answer any questions or concerns you have about keeping your personal information safe.

IDX
A ZEROFOX COMPANY

**Recommended Steps to help Protect your Information**

1. **Telephone.** Contact IDX at 1-877-229-9277 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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

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

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

**Credit Bureaus**

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

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

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

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

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

**California Residents:** Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Community Health Center, Inc.
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/CommunityHealthCenter

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

January 30, 2025

**Notice of Data Breach**

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

You are receiving this letter because you received a COVID test and/or COVID vaccination at a clinic operated by Community Health Center, Inc. ("CHC"). We are writing to inform you of a data security incident that may have exposed your personal information. We take your privacy seriously, so we want to share details of the incident and how you can protect your personal information.

**What Happened**

On January 2, 2025, we noticed unusual activity in our computer systems. That same day, we brought in experts to investigate and reinforce the security of our systems. They found that a skilled criminal hacker got into our system and took some data, which might include your personal information. Fortunately, the criminal hacker did not delete or lock any of our data, and the criminal's activity did not affect our daily operations. We believe we stopped the criminal hacker's access within hours, and that there is no current threat to our systems.

**What Information Was Involved**

If you received COVID testing or vaccine services from CHC, the personal information that may have been impacted includes name, date of birth, phone number, email, address, gender, race, ethnicity, and Social Security Number. For testing only patients, the date of test and result information was also involved. For vaccine patients, health insurance information, guarantor name and vaccine type, dose and date administered may also have been involved.

**What We Are Doing**

We've strengthened our security and added special software to watch for suspicious activity. We are also working to make sure your information stays safe in the future.

So far, there is no sign that your information has been misused. To help protect you, we're offering free identity theft protection through IDX. IDX is a company that we've hired to help protect you and answer your questions. These services include:

- 24 months of credit and CyberScan monitoring
- A $1,000,000 insurance reimbursement policy
- Help recovering your identity if it is stolen

IDX
A ZEROFOX COMPANY

**Recommended Steps to help Protect your Information**

**1. Website and Enrollment.** Go to https://response.idx.us/CommunityHealthCenter and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

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

**3. Telephone.** Contact IDX at 1-877-229-9277 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

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

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

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

**Credit Bureaus**

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

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

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

**6. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place

Community Health Center, Inc.
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/CommunityHealthCenter

To the Parent or Guardian of
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

January 30, 2025

**Notice of Data Breach**

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

You are receiving this letter because your child received a COVID test and/or COVID vaccination at a clinic operated by Community Health Center, Inc. ("CHC"). We are writing to inform you of a data security incident that may have exposed your child's personal information. We take your child's privacy seriously, so we want to share details of the incident and how you can protect your child's personal information.

**What Happened**

On January 2, 2025, we noticed unusual activity in our computer systems. That same day, we brought in experts to investigate and reinforce the security of our systems. They found that a skilled criminal hacker got into our system and took some data, which might include your child's personal information. Fortunately, the criminal hacker did not delete or lock any of our data, and the criminal's activity did not affect our daily operations. We believe we stopped the criminal hacker's access within hours, and that there is no current threat to our systems.

**What Information Was Involved**

If your child received COVID testing or vaccine services from CHC, the personal information that may have been impacted includes your child's name, date of birth, phone number, email, address, gender, race, ethnicity, and Social Security Number. For testing only patients, the date of test and result information was also involved. For vaccine patients, health insurance information, guarantor name and vaccine type, dose and date administered may also have been involved.

**What We Are Doing**

We've strengthened our security and added special software to watch for suspicious activity. We are also working to make sure your information stays safe in the future.

So far, there is no sign that your child's information has been misused. To help protect you, we're offering free identity theft protection through IDX. IDX is a company that we've hired to help protect you and answer your questions. These services include:

- 24 months of CyberScan monitoring
- A $1,000,000 insurance reimbursement policy
- Help recovering your identity if it is stolen

IDX
A ZEROFOX COMPANY

**Recommended Steps to help Protect your Information**

**1. Website and Enrollment.** Go to https://response.idx.us/CommunityHealthCenter and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

**2. Telephone.** Contact IDX at 1-877-229-9277 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

**3. Watch for Suspicious Activity.** If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

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

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

**4. Security Freeze.** You may place a free credit freeze for children under age 16. By placing a security freeze, someone who fraudulently acquires your child's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the three national credit reporting bureaus listed below to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your child's credit files.

**Credit Bureaus**

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

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

**California Residents:** Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

**Connecticut Residents:** The Attorney General may be contacted at: 165 Capitol Avenue, Hartford, CT 06106; 1-860-808-5318; https://portal.ct.gov/AG.

**District of Columbia:** Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

**Iowa Residents:** You should report any suspected identity theft to law enforcement or to the Iowa Attorney General, Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Community Health Center, Inc.
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/CommunityHealthCenter

To the Next of Kin of:
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

January 30, 2025

**Notice of Data Breach**

Dear Next of Kin of <<First Name>> <<Last Name>>,

You are receiving this letter because you are listed as the next of kin or personal representative of a patient of Community Health Center, Inc. ("CHC") who is deceased. Please accept our condolences and apologies for this intrusion at a difficult time. We are writing to inform you of a data security incident that may have exposed the personal information of the deceased patient. We take privacy seriously, so we want to share details of the incident and how you can protect the deceased patient's personal information.

**What Happened**

On January 2, 2025, we noticed unusual activity in our computer systems. That same day, we brought in experts to investigate and reinforce the security of our systems. They found that a skilled criminal hacker got into our system and took some data, which might include your personal information. Fortunately, the criminal hacker did not delete or lock any of our data, and the criminal's activity did not affect our daily operations. We believe we stopped the criminal hacker's access within hours, and that there is no current threat to our systems.

**What Information Was Involved**

The deceased patient's personal information that may have been accessed or taken includes all information in the patient's CHC medical record, including name, date of birth, address, phone, email, diagnoses, progress notes, medications, treatment information, test results, records received from other providers, Social Security Number, and health insurance information.

**What We Are Doing**

We've strengthened our security and added special software to watch for suspicious activity. We are also working to make sure our patients' information stays safe in the future.

So far, there is no sign that this information has been misused. To help protect the information, we're offering free identity theft protection through IDX. IDX is a company that we've hired to provide protection and answer your questions. These services include:

- 24 months of credit and CyberScan monitoring
- A $1,000,000 insurance reimbursement policy
- Help recovering the deceased patient's identity if it is stolen

IDX
A ZEROFOX COMPANY

**Recommended Steps to help Protect your Information**

**1. Website and Enrollment.** Scan the QR image or go to https://response.idx.us/CommunityHealthCenter and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

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

**3. Telephone.** Contact IDX at 1-877-229-9277 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect the decedent's information.

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

**5. Report suspicious activity.** You have the right to file a police report if identity fraud is experienced. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you are representative to the victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**6. Place Deceased Alerts** with the three credit bureaus. You can place a deceased alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A deceased alert tells creditors to follow certain procedures, including contacting you.

**Credit Bureaus**

| Equifax | Experian | TransUnion |
|---|---|---|
| 1-888-548-7878 | 1-888-397-3742 | 1-800-888-4213 |
| P.O. Box 105139 | P.O. Box 4500 | P.O. Box 2000 |
| Atlanta, GA 30348-5139 | Allen, TX 75013 | Chester, PA 19022-2000 |
| www.equifax.com | www.experian.com | www.transunion.com |

It is necessary to contact only one bureau to provide notification. As soon as one of the three bureaus confirms your deceased alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail.

**7. Security Freeze.** By placing a security freeze, someone who fraudulently acquires the decedent's personal identifying information will not be able to use that information to open new accounts or borrow money in the decedent's name. You will need to contact the three national credit reporting bureaus listed above to place the freeze.

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

**California Residents:** Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Community Health Center, Inc.
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/CommunityHealthCenter

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

January 30, 2025

**Notice of Data Breach**

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

You are receiving this letter because you are listed as a guarantor or person who provided insurance for a current or former patient of Community Health Center, Inc. ("CHC"). We are writing to inform you of a data security incident that may have exposed your personal information. We take privacy seriously, so we want to share details of the incident and how you can protect your personal information.

**What Happened**

On January 2, 2025, we noticed unusual activity in our computer systems. That same day, we brought in experts to investigate and reinforce the security of our systems. They found that a skilled criminal hacker got into our system and took some data, which might include your personal information. Fortunately, the criminal hacker did not delete or lock any of our data, and the criminal's activity did not affect our daily operations. We believe we stopped the criminal hacker's access within hours, and that there is no current threat to our systems.

**What Information Was Involved**

You were listed as a "guarantor" or "insured other" for a current or former patient of CHC in the patient's health record. For example, you may be a parent or legal guardian of a minor patient or you may hold insurance coverage that applies to a patient. The personal information about you that may have been involved includes your name, address, phone number, email address, Social Security Number, and insurance information.

**What We Are Doing**

We've strengthened our security and added special software to watch for suspicious activity. We are also working to make sure your information stays safe in the future.

So far, there is no sign that your information has been misused. To help protect you, we're offering free identity theft protection through IDX. IDX is a company that we've hired to help protect you and answer your questions. These services include:

- 24 months of credit and CyberScan monitoring
- A $1,000,000 insurance reimbursement policy
- Help recovering your identity if it is stolen

IDX
A ZEROFOX COMPANY

**Recommended Steps to help Protect your Information**

**1. Website and Enrollment.** Go to https://response.idx.us/CommunityHealthCenter and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

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

**3. Telephone.** Contact IDX at 1-877-229-9277 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

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

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

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

**Credit Bureaus**

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

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

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

**6. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place