

2024-166

INHEALTH

TECHNOLOGIES®

P.O. Box 989728

West Sacramento, CA 95798-9728

Enrollment Code: <<Enrollment Code>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

January 9, 2024

Notice of Data Breach

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

The protection of your personal information is a priority at InHealth Technologies (“InHealth”). We are writing to inform you of a security incident that may have involved your personal information. We take this matter very seriously and understand the personal nature of the information at issue. The security of your information is of the highest importance to us, and we are handling this incident with the greatest of care. At this time, there is no evidence of any attempt to misuse any of your information.

What Happened

On November 11, 2023, we became aware of an incident in which unauthorized personnel accessed and attempted to disable certain InHealth systems. During the incident, certain files were encrypted and potentially accessed by an unauthorized party. Immediately after discovery, InHealth began an investigation in conjunction with outside consultants to investigate the incident and remediate its effects.

What Information Was Involved

In the incident, personal health information exposed may have included your: name, date of birth, and demographic information at enrollment; social security number; prescription information, including prescribing physician, diagnostic code, and products prescribed/purchased from us; and health insurance/billing information and details.

What We Are Doing

We take this event, your privacy, and the security of information in our care very seriously. Upon learning of the suspicious activity, InHealth moved immediately to investigate and respond. The investigation included confirming the security of our network, restoring affected systems, and determining the extent of personal and personal health information potentially affected. We have also hardened our existing data security with additional access controls, further data minimization, and supplemental monitoring tools, in order to prevent attacks from occurring in the future.

In addition, we are offering complimentary identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: <<12 months/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

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by going to <https://app.idx.us/account-creation/protect> or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is April 9, 2024.

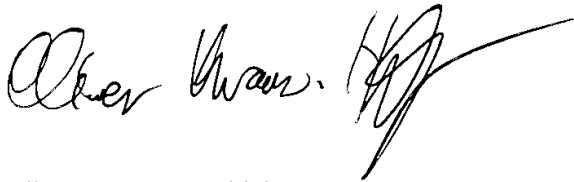
Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

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

Please call (888) 903-5490 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

A handwritten signature in black ink, appearing to read "Oliver Krause-Huckleberry". The signature is stylized and includes a long horizontal flourish extending to the right.

Oliver Krause-Huckleberry
Vice President & General Manager
InHealth Technologies

(Enclosure)



Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Scan the QR image or go to <https://app.idx.us/account-creation/protect> 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 (888) 903-5490 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
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

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

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

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

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

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

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

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

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

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

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

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

INHEALTH

TECHNOLOGIES®

P.O. Box 989728

West Sacramento, CA 95798-9728

Personal Representative of

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

January 9, 2024

Notice of Data Breach

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

The protection of personal information is a priority at InHealth Technologies (“InHealth”). We are writing to inform you of a security incident that may have involved the above-named decedent’s personal information. We take this matter very seriously and understand the personal nature of the information at issue. The security of the decedent’s information is of the highest importance to us, and we are handling this incident with the greatest of care. At this time, there is no evidence of any attempt to misuse any of the decedent’s information.

What Happened

On November 11, 2023, we became aware of an incident in which unauthorized personnel accessed and attempted to disable certain InHealth systems. During the incident, certain files were encrypted and potentially accessed by an unauthorized party. Immediately after discovery, InHealth began an investigation in conjunction with outside consultants to investigate the incident and remediate its effects.

What Information Was Involved

In the incident, personal health information exposed may have included the decedent’s name, date of birth, and demographic information at enrollment; social security number; prescription information, including prescribing physician, diagnostic code, and products prescribed/purchased from us; and health insurance/billing information and details.

What We Are Doing

We take this event, privacy, and the security of information in our care very seriously. Upon learning of the suspicious activity, InHealth moved immediately to investigate and respond. The investigation included confirming the security of our network, restoring affected systems, and determining the extent of personal and personal health information potentially affected. We have also hardened our existing data security with additional access controls, further data minimization, and supplemental monitoring tools, in order to prevent attacks from occurring in the future.

What You Can Do

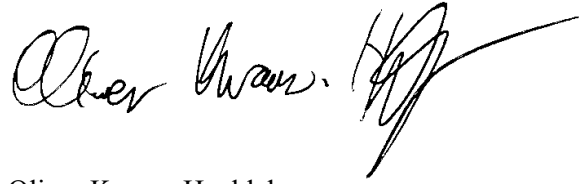
We have partnered with IDX, A ZeroFox Company to answer questions and provide valuable information about the incident. We encourage you to contact IDX with any questions by calling (888) 903-5490. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time.

For More Information

You will find additional information in the enclosed Recommended Steps document.

Please call (888) 903-5490 for any additional questions you may have.

Sincerely,

A handwritten signature in black ink, appearing to read "Oliver Krause-Huckleberry". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Oliver Krause-Huckleberry
Vice President & General Manager
InHealth Technologies

(Enclosure)



Recommended Steps to help Protect the Decedent's Information

1. Telephone. Contact IDX at (888) 903-5490 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect the decedent's information.

2. 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.

3. 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.

4. 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
1-888-548-7878
P.O. Box 105139
Atlanta, GA 30348-5139
www.equifax.com

Experian
1-888-397-3742
P.O. Box 4500
Allen, TX 75013
www.experian.com

TransUnion
1-800-888-4213
P.O. Box 2000
Chester, PA 19022-2000
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.

5. 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.

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.

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

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable

information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

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

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

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

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