



C/O IDX
PO Box 4129
Everett WA 98204

ENDORSE



NAME

ADDRESS1

ADDRESS2

CSZ

COUNTRY



SEQ
CODE 2D
Ver A

BREAK

To Enroll, Please Call:

833-903-3647

Or Visit:

<https://response.idx.us/holdings>

Enrollment Code: <<XXXXXXXXXX>>

March 31, 2021

Notice of Data Security Incident

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

We are writing to inform you of a data security incident experienced by Med-Data, Incorporated (“Med-Data”) that may have impacted your protected health information (“PHI”) described below. Med-Data provides revenue cycle services to hospitals and healthcare systems and their patients, including solutions for Medicaid eligibility, third-party liability, workers’ compensation, and patient billing. Med-Data has your information because we assisted <<Covered Entity name/Mod Text Field 1>> with processing your claim. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

What happened:

On December 10, 2020, an independent journalist informed Med-Data that some data related to its business had been uploaded to a public-facing website (“the Website”). On December 14, 2020, the journalist provided a link to the data, and Med-Data immediately launched an internal investigation to validate the journalist’s claim and discovered that a former employee had saved files to personal folders they created on the Website sometime between December 2018 and September 2019 while employed with Med-Data. The files were promptly removed from the Website on December 17, 2020.

Med-Data hired cybersecurity specialists to assist in the review of the files to determine what information may have been included. Further review confirmed that the files may have contained PHI for patients whose information may have been processed by Med-Data. The cybersecurity specialists conducted an in-depth review of the files to identify PHI and extract contact information of potentially affected individuals. On February 5, 2021, the cybersecurity specialists completed their review and provided Med-Data a list of impacted individuals, and we determined that your PHI may have been impacted by this incident.

What information was involved:

The investigation concluded that the files may have contained your <<include applicable PHI identifiers for impacted individual/Mod Text Field 2>>. Your electronic health record and information stored with <<Covered Entity name/Mod Text Field 1>> were not affected by this incident and remain secure.

What we are doing:

Med-Data takes this incident and the security of your personal information seriously. To minimize the risk of this happening in the future, we have implemented additional security controls, blocked all file sharing websites, updated internal data policies and procedures, implemented a security operations center, and deployed a managed detection and response solution that provides 24x7 monitoring of our network, endpoints, and workstations.

In addition, while we are not aware of any misuse of your information, we have arranged for you to receive credit monitoring and identity protection services at no cost to you, as a precautionary measure.

What you can do:

We are offering identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: xx 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.

We encourage you to remain vigilant against incidents of identity theft by reviewing account statements and explanations of benefits for unusual activity. You should immediately report any suspicious activity to your insurance company, healthcare provider, or financial institution.

How to Enroll in IDX: You can sign up online or via telephone

We encourage you to contact IDX with any questions and to enroll in free services by calling 833-903-3647 or going to <https://response.idx.us/holdings> and using the Enrollment Code provided above. IDX is available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is July 1, 2021.

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 informed of the incident and can answer questions or concerns you may have regarding protection of your personal information.

For more information:

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

Please call 833-903-3647 or go to <https://response.idx.us/holdings> for assistance or for any additional questions you may have.

Your trust is a top priority for us, and we sincerely apologize for any concern or inconvenience this may cause you.

Sincerely,



Michael Shea
Chief Executive Officer
Med-Data, Incorporated



Recommended Steps to help Protect your Information

- 1. Website and Enrollment.** Go to <https://response.idx.us/holdings> 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 833-903-3647 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.

Connecticut: your state Attorney General may be contacted at: Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

District of Columbia: your state Attorney General may be contacted at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

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.

Massachusetts: your state Attorney General may be contacted at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

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


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

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

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


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

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



C/O IDX
 PO Box 4129
 Everett WA 98204

ENDORSE



To the Parent or Guardian of
 NAME
 ADDRESS1
 ADDRESS2
 CSZ
 COUNTRY

SEQ
 CODE 2D
 Ver C

BREAK

To Enroll, Please Call:
 833-903-3647
 Or Visit:
<https://response.idx.us/holdings>
 Enrollment Code: <<XXXXXXXXXX>>

March 31, 2021

Notice of Data Security Incident

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

We are writing to inform you of a data security incident experienced by Med-Data, Incorporated (“Med-Data”) that may have impacted your dependent’s protected health information (“PHI”) described below. Med-Data provides revenue cycle services to hospitals and healthcare systems and their patients, including solutions for Medicaid eligibility, third-party liability, workers’ compensation, and patient billing. Med-Data has your dependent’s information because we assisted <<Covered Entity name/Mod Text Field 1>> with processing their claim. This letter contains information about steps you can take to protect their information and resources we are making available to help you.

What happened:

On December 10, 2020, an independent journalist informed Med-Data that some data related to its business had been uploaded to a public-facing website (“the Website”). On December 14, 2020, the journalist provided a link to the data, and Med-Data immediately launched an internal investigation to validate the journalist’s claim and discovered that a former employee had saved files to personal folders they created on the Website sometime between December 2018 and September 2019 while employed with Med-Data. The files were promptly removed from the Website on December 17, 2020.

Med-Data hired cybersecurity specialists to assist in the review of the files to determine what information may have been included. Further review confirmed that the files may have contained PHI for patients whose information may have been processed by Med-Data. The cybersecurity specialists conducted an in-depth review of the files to identify PHI and extract contact information of potentially affected individuals. On February 5, 2021, the cybersecurity specialists completed their review and provided Med-Data a list of impacted individuals, and we determined that your dependent’s PHI may have been impacted by this incident.

What information was involved:

The investigation concluded that the files may have contained your dependent’s <<include applicable PHI identifiers for impacted individual/Mod Text Field 2>>. Your dependent’s electronic health record and information stored with <<Covered Entity name/Mod Text Field 1>> were not affected by this incident and remain secure.

What we are doing:

Med-Data takes this incident and the security of your dependent’s personal information seriously. To minimize the risk of this happening in the future, we have implemented additional security controls, blocked all file sharing websites, updated internal data policies and procedures, implemented a security operations center, and deployed a managed detection and response solution that provides 24x7 monitoring of our network, endpoints, and workstations.

In addition, while we are not aware of any misuse of your dependent's information, we have arranged for your dependent to receive identity protection services at no cost to you, as a precautionary measure.

What you can do:

We are offering identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: xx 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 identity is compromised.

We encourage you to remain vigilant against incidents of identity theft by reviewing account statements and explanations of benefits for unusual activity. You should immediately report any suspicious activity to your insurance company, healthcare provider, or financial institution.

How to Enroll in IDX: You can sign up online or via telephone

We encourage you to contact IDX with any questions and to enroll in free services by calling 833-903-3647 or going to <https://response.idx.us/holdings> and using the Enrollment Code provided above. IDX is available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is July 1, 2021.

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

For more information:

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

Please call 833-903-3647 or go to <https://response.idx.us/holdings> for assistance or for any additional questions you may have.

Your trust is a top priority for us, and we sincerely apologize for any concern or inconvenience this may cause you.

Sincerely,



Michael Shea
Chief Executive Officer
Med-Data, Incorporated



Recommended Steps to help Protect your Dependent's Information

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

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

3. Telephone. Contact IDX at 833-903-3647 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your dependent's identity.

4. Watch for Suspicious Activity. If you discover any suspicious items and have enrolled your dependent 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 on your dependent's behalf, 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 your dependent falls victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your dependent's behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report on your dependent's behalf if there is 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 your dependent has 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. 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 existing accounts. 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 dependent's 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 dependent's credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your dependent'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 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 in your dependent's name until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your dependent's credit file.

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.

Connecticut: your state Attorney General may be contacted at: Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

District of Columbia: your state Attorney General may be contacted at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

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.

Massachusetts: your state Attorney General may be contacted at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

New Mexico Residents: You and your dependent have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your dependent's credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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; and access to your dependent's file is limited. You and your dependent may have additional rights under the Fair Credit Reporting Act not summarized here. You can review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

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

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

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

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