Arietis Health
RCM REIMAGINED

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

<<Variable Header - Notice of Data Breach/Notice of Security Incident>>

Dear <<Name 1>>,

We write to inform you of a recent data security incident that may have involved some of your information. Arietis Health LLC ("Arietis Health") received that information in connection with healthcare billing services it provides to <<Variable Data – BillingEntity>>, which administered pain management services or anesthesia in connection with medical treatment you received from your healthcare provider. Arietis Health is one of thousands of organizations worldwide that may have recently been affected by the MOVEit software vulnerability. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your information.

What Happened? On May 31, 2023, Progress Software – the company responsible for MOVEit software – alerted Arietis Health to a critical vulnerability affecting MOVEit, a solution used widely by businesses and government agencies, including Arietis Health, to securely transfer data. After becoming aware of the alert, Arietis Health took immediate steps to secure and patch its MOVEit server in accordance with Progress Software's instructions. Arietis Health thereafter engaged leading, independent cybersecurity experts to conduct a comprehensive investigation. On July 26, 2023, the investigation determined that unauthorized actors had access to Arietis Health's MOVEit server on May 31, 2023, and may have acquired certain files which contained your data. On August 3, 2023, Arietis Health informed <<Variable Data – BillingEntity>> of the incident, and reviewed the impacted data to determine what information may have been involved in the incident.

What Information Was Involved? The information potentially impacted in connection with this incident may have included your name as well as your <<Breached Elements>>.

What Are We Doing? As soon as Arietis Health discovered the incident, Arietis Health took the steps described above. In addition, Arietis Health is providing you with information about steps that you can take to help protect your information. Furthermore, to help relieve concerns and restore confidence following this incident, Arietis Health has engaged CyEx to provide complimentary Identity Monitoring services for <<12/24>> months. CyEx is a global leader in risk mitigation and response, and the CyEx team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

What You Can Do: Arietis Health recommends that you review the guidance included with this letter about how to help protect your information. We also encourage you to activate the Identity Monitoring services being offered to you through CyEx, which are free to you upon activation. You will need to reference the CyEx membership number in this letter when enrolling, so please do not discard this letter.

Visit https://app.medicalshield.cyex.com/enrollment/activate/arie to activate and take advantage of your Identity Monitoring services.

You have until **<<Enrollment Deadline>>** to activate your credit and identity monitoring services.

Membership Number: **<<Activation Code>>**

For more information about CyEx and your Identity Monitoring services, you can visit app.medicalshield.cyex.com/enrollment/activate/. Additional information describing your services is included with this letter.

For more information. If you have any questions about this incident or the complimentary services being offered to you, please contact our dedicated call center at 855-657-4306, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays. Please have your membership number ready.

We take the privacy and security of all information within our possession very seriously. Please accept our sincere apologies and know that Arietis Health deeply regrets any worry or inconvenience that this may cause you.

Sincerely,
Ashwini Kotwal
Ashwini Kotwal
Founder and CEO
Arietis Health, LLC

Medical Shield Complete

Key Features

- <<12/24>> month service term*
- 1-Bureau Credit Monitoring
- Health Insurance Plan Number Monitoring
- Medical Record Number Monitoring
- Medical Beneficiary Identifier Monitoring
- National Provider Number Monitoring
- International Classification of Diseases Monitoring
- Health Savings Account Monitoring
- Dark Web Monitoring
- Victim Assistance
- $1 Million Identity Theft Insurance**

Enrollment Instructions

To enroll in Medical Shield, visit https://app.medicalshield.cyex.com/enrollment/activate/arie.

1. Enter your unique Membership Number: **<<Activation Code>>**
   Enter your Membership Number and click 'Redeem Code'.
2. Create Your Account
   Enter your email address, create your password, and click 'Create Account'.
3. Register
   Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. Complete Activation
   Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Medical Shield code will no longer be active. **If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Medical Shield, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Medical Shield, please call Medical Shield directly at 1.855.727.5798.

---

* Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.

** Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 1000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 160, Woodlyn, PA 19094, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com
  You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request. If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

District of Columbia: You may contact and obtain information from your attorney general 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.

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us.

Massachusetts: Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general 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 York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Center, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov.

Rhode Island: Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.
- You have a right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

Arietis Health
RCM REIMAGINED

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
Parent or Guardian of
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

<<Variable Header - Notice of Data Breach/Notice of Security Incident>>

Dear Parent or Guardian of <<Name 1>>,

We write to inform you of a recent data security incident that may have involved some of your minor's information. Arietis Health LLC ("Arietis Health") received that information in connection with healthcare billing services it provides to <<Variable Data – BillingEntity>>, which administered pain management services or anesthesia in connection with medical treatment your minor received from their healthcare provider. Arietis Health is one of thousands of organizations worldwide that may have recently been affected by the MOVEit software vulnerability. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your minor's information.

What Happened? On May 31, 2023, Progress Software – the company responsible for MOVEit software – alerted Arietis Health to a critical vulnerability affecting MOVEit, a solution used widely by businesses and government agencies, including Arietis Health, to securely transfer data. After becoming aware of the alert, Arietis Health took immediate steps to secure and patch its MOVEit server in accordance with Progress Software's instructions. Arietis Health thereafter engaged leading, independent cybersecurity experts to conduct a comprehensive investigation. On July 26, 2023, the investigation determined that unauthorized actors had access to Arietis Health's MOVEit server on May 31, 2023, and may have acquired certain files which contained your minor's data. On August 3, 2023, Arietis Health informed <<Variable Data – BillingEntity>> of the incident, and reviewed the impacted data to determine what information may have been involved in the incident.

What Information Was Involved? The information potentially impacted in connection with this incident may have included your minor's name as well as their <<Breached Elements>>.

What Are We Doing? As soon as Arietis Health discovered the incident, Arietis Health took the steps described above. In addition, Arietis Health is providing you with information about steps that you can take to help protect your minor's information. Furthermore, to help relieve concerns and restore confidence following this incident, Arietis Health has engaged CyEx to provide complimentary Identity Monitoring services for <<12/24>> months. CyEx is a global leader in risk mitigation and response, and the CyEx team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

What You Can Do: Arietis Health recommends that you review the guidance included with this letter about how to help protect your minor's information. We also encourage you to activate the Identity Monitoring services being offered to your minor through CyEx, which are free to your minor upon activation. You will need to reference the CyEx membership number in this letter when enrolling, so please do not discard this letter.

Visit https://app.minordefense.com/enrollment/activate/ariemd to activate and take advantage of your minor's Identity Monitoring services.

You have until **<<Enrollment Deadline>>** to activate your minor's identity monitoring services.

Membership Number: **<<Activation Code>>**

For more information about **CyEx** and your minor's Identity Monitoring services, you can visit https://app.minordefense.cyex.com/enrollment/activate/. Additional information describing your services is included with this letter.

For more information. If you have any questions about this incident or the complimentary services being offered to your minor, please contact our dedicated call center at 855-657-4306, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays. Please have your membership number ready.

We take the privacy and security of all information within our possession very seriously. Please accept our sincere apologies and know that Arietis Health deeply regrets any worry or inconvenience that this may cause you.

Sincerely,
Ashwini Kotwal
Ashwini Kotwal
Founder and CEO
Arietis Health, LLC

Minor Defense

Key Features

- <<12/24>> month service term*
- Synthetic Identity Monitoring
- Public Record Trace
- Dark Web Monitoring
- Parent/Custodial Adult Controls
- Victim Assistance

Enrollment Instructions
To enroll in Minor Defense, visit https://app.minordefense.com/enrollment/activate/ariemd.

1. Enter your unique Membership Number: **<<Activation Code>>**
   If you received more than one code to enroll more than one minor, please enter one code to enroll yourself first.
2. Create Your Account
   Enter your email address, create your password, and click 'Create Account'.
3. Register
   Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. Complete Activation
   Click 'Continue to Dashboard' to finish enrolling.
5. Enroll Eligible Minors
   To enroll your first minor, enter the same code that you used to enroll yourself. Once you enroll your first minor, you will not be able to use that same code again. To enroll additional minors, please enter additional codes one time each.

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Minor Defense code will no longer be active. **If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Minor Defense, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Minor Defense, please call Minor Defense directly at 1.855.677.6672.

---

* Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your child's account statements and free credit reports for any unauthorized activity. Parents or guardians may request a copy of their child's or ward's credit information by contacting the three credit reporting bureaus. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 1000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe your child is the victim of identity theft or have reason to believe your child's personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your child's records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

If your child is a resident of Connecticut, Maryland, Massachusetts, North Carolina, or Rhode Island, you may contact and obtain information from the state attorney general at:

- *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag
- *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us
- *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html
- *North Carolina Attorney General's Office*, 9001 Mail Service Center, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov
- *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

If your child is a resident of Massachusetts or Rhode Island, note that pursuant to Massachusetts or Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

If your child is a resident of New York, you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583/ 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

If your child is a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your child's file to let potential creditors and others know that your child may be a victim of identity theft, as described below. You also have a right to place a security freeze on your child's credit report, as described below.

Fraud Alerts: There are two types of fraud alerts you can place on your child's credit report to put your child's creditors on notice that your child may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your child's credit report if you suspect your child has been, or is about to be, a victim of identity theft. An initial fraud alert stays on your child's credit report for one year. You may have an extended alert placed on your child's credit report if your child has already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your child's credit report for seven years. You can place a fraud alert on your child's credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your child's credit file, free of charge, so that no new credit can be opened in your child's name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your child's credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your child's credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your child's ability to obtain credit. There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your child's credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 160, Woodlyn, PA 19094, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

To request a security freeze, you will need to provide the following information:

1. Your child's full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Your child's Social Security number
3. Your child's date of birth
4. If you have moved in the past five years, provide the addresses where your child has lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If your child is a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your child's credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your child's credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (your child's name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your child's credit report or the specific period of time you want the credit report available. The credit reporting agencies have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (your child's name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze. The credit bureaus have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.