Xsolis, Inc.

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

SCAN TO ENROLL

<<Date>> (Format: Month Day, Year)

Notice of Data Breach

Dear <<First_name>> <<Last_name>>,

Your healthcare provider values the opportunity to provide services to you, and they take their responsibility to protect the information you share with them seriously. We are writing to tell you about a data security incident that may have exposed some of your personal information.

What happened?

Your healthcare provider uses a vendor, Xsolis, Inc. ("Xsolis"), to provide certain case and utilization management services. Xsolis recently informed your healthcare provider of certain unauthorized activity impacting a limited portion of their environment.

Xsolis became aware of unauthorized activity resulting from a targeted phishing attack on January 22, 2026. Upon discovering the unauthorized activity, Xsolis immediately interrupted and contained the issue and terminated the unauthorized access.

As part of its response and investigation, Xsolis engaged external cybersecurity experts and notified law enforcement. There has been no evidence of unauthorized activity within the Xsolis environment since January 22, 2026. Additionally, there is no evidence of any misuse of the impacted data.

What information was involved?

We worked diligently with consultants to assess the data and identify any affected protected health information. We are notifying you of this incident because we have determined that some of your information may have been accessed, which may have included your <<b2b_text_2 (Data Elements)>>. Although we have no evidence that the information involved in this incident has been improperly used, we recommend that you remain vigilant against fraud and identity theft.

What we are doing.

Immediately upon discovering the incident, Xsolis launched an investigation and undertook immediate mitigation steps to eliminate the threat. Since then, Xsolis has implemented additional security measures, including resetting passwords for all users and key accounts, increasing monitoring of systems, deploying new protective technology, completing the rollout of updated security measures, accelerating annual security training for employees, and strengthening processes for managing credentials and responding to future incidents. We continue to work with security professionals to reinforce the security of our digital environment.

We want you to feel confident that your data is secure. To help protect your identity, we are offering you the services of Kroll to provide identity monitoring at no cost for twelve (12) months. Kroll is a global leader in risk mitigation and r esponse, and their team has extensive experience helping people who have sustained an unintentional exposure of con fidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Rest oration.

To enroll in these services at no charge, please visit **Enroll.krollmonitoring.com/redeem** and follow the instructions provided. When prompted, please provide the following unique code: **<<b2b_text_5 (Activation Code)>>** and Verification ID: **<<b2b_text_4 (Verification ID)>>** to access your services. For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

To receive the services described in this letter, you must enroll by **<<b2b_text_6 (activation deadline)>>**. Please note that enrollment requires an internet connection and may not be available to minors under the age of 18.

What you can do.

Although we have no evidence that any of your information has been subject to identity theft or fraud, you should always remain alert by regularly reviewing your account statements and monitoring your free credit reports. Please immediately report any suspicious activity to your banks and other financial institutions. We also encourage you to enroll in the identity monitoring services that we have offered to you.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please contact us at (844) 403-4585 Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction. We deeply regret any inconvenience that this incident may have caused.

Sincerely,

Xsolis, Inc.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. We recommend that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud or identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alerts. There are two types of 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 at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. 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 home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

State-Specific Information:

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Rhode Island, and Puerto Rico residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/, 1-888-743-0023.

New Mexico residents: New Mexico consumers have the right to obtain a security freeze or submit a declaration of removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;

(2) proper identification to verify your identity; and

(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone. A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act. If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For New York residents: You may contact the New York Attorney General at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/. Additional information is available at the New York Department of State Division of Consumer Protection website, https://ag.ny.gov/consumer-frauds-bureau/identity-theft.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226 or 1-919-716-6000.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1-401-274-4400. You have the right to file or obtain a police report. You have the right to request a security freeze as described above.

For South Carolina residents: You may contact the South Carolina Department of Consumer Affairs at 1-800-922-1594 for guidance on preventing and minimizing the effects of identity theft.

For District of Columbia residents: You may contact the Office of Attorney General for the District of Columbia, Office of Consumer Protection, 400 6th Street NW, Washington, DC 20001; https://oag.dc.gov/; 1-202-727-3400 or 1-202-442-9828.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Fraud Consultation. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Xsolis, Inc.

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

PARENT/GUARDIAN OF
<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

<<Date>> (Format: Month Day, Year)

Notice of Data Breach

Dear Parent or Guardian of <<First_name>> <<Last_name>>,

Your healthcare provider values the opportunity to provide services to your child, and they take their responsibility to protect your child's information seriously. We are writing to tell you about a data security incident that may have exposed some of your child's personal information.

What happened?

Your healthcare provider uses a vendor, Xsolis, Inc. ("Xsolis"), to provide certain case and utilization management services. Xsolis recently informed your healthcare provider of certain unauthorized activity impacting a limited portion of their environment.

Xsolis became aware of unauthorized activity resulting from a targeted phishing attack on January 22, 2026. Upon discovering the unauthorized activity, Xsolis immediately interrupted and contained the issue and terminated the unauthorized access.

As part of its response and investigation, Xsolis engaged external cybersecurity experts and notified law enforcement. There has been no evidence of unauthorized activity within the Xsolis environment since January 22, 2026. Additionally, there is no evidence of any misuse of the impacted data.

What information was involved?

We worked diligently with consultants to assess the data and identify any affected protected health information. We are notifying you of this incident because we have determined that some of your child's information may have been accessed, which may have included your child's <<b2b_text_2 (Data Elements)>>. Although we have no evidence that the information involved in this incident has been improperly used, we recommend that you remain vigilant against fraud and identity theft.

What we are doing.

Immediately upon discovering the incident, Xsolis launched an investigation and undertook immediate mitigation steps to eliminate the threat. Since then, Xsolis has implemented additional security measures, including resetting passwords for all users and key accounts, increasing monitoring of systems, deploying new protective technology, completing the rollout of updated security measures, accelerating annual security training for employees, and strengthening processes for managing credentials and responding to future incidents. We continue to work with security professionals to reinforce the security of our digital environment.

We want you to feel confident that your child's data is secure. To help protect your child's identity, we are offering your child Minor Identity Monitoring by Kroll at no cost for twelve (12) months. Kroll is a global leader in risk mitigation a nd response, and their team has extensive experience helping people who have sustained an unintentional exposure of con fidential data. Minor Identity Monitoring services include Minor Identity Monitoring, Fraud Consultation,

and Identity Theft Restoration.

To enroll in Minor Identity Monitoring services at no charge, please visit **Enroll.krollmonitoring.com/redeem** and follow the instructions provided. When prompted, please provide the following unique code: **<<b2b_text_5 (Activation Code)>>** and Verification ID: **<<b2b_text_4 (Verification ID)>>** to access your child's Minor Identity Monitoring services. For more information about Kroll and your child's Minor Identity Monitoring services, you can visit info.krollmonitoring.com.

To receive the services described in this letter, you must enroll by **<<b2b_text_6 (activation deadline)>>**. Please note that enrollment requires an internet connection.

What you can do.

We have no evidence that any of your child's information has been subject to identity theft or fraud. However, please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect your child's identity, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your child's credit file. We also encourage you to enroll your child in the Minor Identity Monitoring services that we have offered.

For more information.

If you have questions, please contact us at (844) 403-4585 Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your child's membership number ready.

Protecting your child's information is important to us. We trust that the services we are offering to your child demonstrate our continued commitment to your security and satisfaction. We deeply regret any inconvenience that this incident may have caused.

Sincerely,

Xsolis, Inc.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. We recommend that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud or identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alerts. There are two types of 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 at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. 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 home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

State-Specific Information:

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Rhode Island, and Puerto Rico residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/, 1-888-743-0023.

New Mexico residents: New Mexico consumers have the right to obtain a security freeze or submit a declaration of removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;

(2) proper identification to verify your identity; and

(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone. A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act. If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For New York residents: You may contact the New York Attorney General at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/. Additional information is available at the New York Department of State Division of Consumer Protection website, https://ag.ny.gov/consumer-frauds-bureau/identity-theft.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226 or 1-919-716-6000.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1-401-274-4400. You have the right to file or obtain a police report. You have the right to request a security freeze as described above.

For South Carolina residents: You may contact the South Carolina Department of Consumer Affairs at 1-800-922-1594 for guidance on preventing and minimizing the effects of identity theft.

For District of Columbia residents: You may contact the Office of Attorney General for the District of Columbia, Office of Consumer Protection, 400 6th Street NW, Washington, DC 20001; https://oag.dc.gov/; 1-202-727-3400 or 1-202-442-9828.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Minor Identity Monitoring. Minor Identity Monitoring detects when names, aliases, or addresses become associated with your child's Social Security number. An alert will be sent to you when activity is detected. The presence of a credit file may be an indicator of identity theft or fraud for children who, as minors, should not have a credit history. To activate services, a U.S. Social Security number and U.S. residential address is required.

Fraud Consultation. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Xsolis, Inc.

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

TO THE ESTATE/NEXT OF KIN OF:
<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

<<Date>> (Format: Month Day, Year)

Notice of Data Breach

Dear Personal Representative/Next of Kin of <<First_name>> <<Last_name>>,

Your healthcare provider values the opportunity to have provided services to your loved one, and they take their responsibility to protect their information seriously. We are writing to tell you about a data security incident that may have exposed some of their personal information.

What happened?

Your healthcare provider uses a vendor, Xsolis, Inc. ("Xsolis"), to provide certain case and utilization management services. Xsolis recently informed your healthcare provider of certain unauthorized activity impacting a limited portion of their environment.

Xsolis became aware of unauthorized activity resulting from a targeted phishing attack on January 22, 2026. Upon discovering the unauthorized activity, Xsolis immediately interrupted and contained the issue and terminated the unauthorized access.

As part of its response and investigation, Xsolis engaged external cybersecurity experts and notified law enforcement. There has been no evidence of unauthorized activity within the Xsolis environment since January 22, 2026. Additionally, there is no evidence of any misuse of the impacted data.

What information was involved?

We worked diligently with consultants to assess the data and identify any affected protected health information. We are notifying you of this incident because we have determined that some of your loved one's information may have been accessed, which may have included their <<b2b_text_2 (Data Elements)>>. Although we have no evidence that the information involved in this incident has been improperly used, we recommend that you remain vigilant against fraud and identity theft, should you feel it appropriate.

What we are doing.

Immediately upon discovering the incident, Xsolis launched an investigation and undertook immediate mitigation steps to eliminate the threat. Since then, Xsolis has implemented additional security measures, including resetting passwords for all users and key accounts, increasing monitoring of systems, deploying new protective technology, completing the rollout of updated security measures, accelerating annual security training for employees, and strengthening processes for managing credentials and responding to future incidents. We continue to work with security professionals to reinforce the security of our digital environment.

What you can do.

We have no evidence that any of your loved one's information has been subject to identity theft or fraud. We encourage you to always remain alert by regularly reviewing your loved one's account statements and monitoring your loved one's free credit reports, if available.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect your loved one's identity.

For more information.

If you have questions, please contact us at (844) 403-4585 Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have this letter available.

Protecting your loved one's information is important to us. We deeply regret any inconvenience that this incident may have caused.

Sincerely,

Xsolis, Inc.

ADDITIONAL RESOURCES

Monitor Your Loved One's Accounts

Authorized individuals, a spouse, or an executor of an estate may request a copy of a loved one's credit report or flag a loved one's credit file with an alert. In most cases, a flag will prevent the opening of new credit accounts in your loved one's name. If you have not already done so, you may request that your loved one's credit report is flagged with the following alert: "Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately: (name and relationship to your loved one)."

Individuals to list in this alert may include:

- next surviving relative, and/or
- another authorized relative, and/or
- executor/trustee of the estate, and/or
- a law enforcement agency.

You may also request a copy of your loved one's credit report to review whether there are any active credit accounts that need to be closed or any pending collection notices that need to be addressed. A request for a flag on your loved one's credit file or for a copy of your loved one's credit report must be in writing and should include the below information:

Information related to your loved one:

- Legal name
- Social Security number
- Date of birth
- Date of death
- Last known address
- A copy of the death certificate or letters testamentary. A "letters testamentary" is a document issued by a court or public official authorizing the executor of a will to take control of a deceased person's estate.

Information related to the individual requesting the information or placing the alert:

- Full name
- Copy of a government issued identification
- Address for sending final confirmation
- In the case of an executor, include the court order or other document indicating the executor of the estate.

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Additional Information. Personal Representatives/Next of Kin may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their loved one's personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that their loved one has been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

State-Specific Information:

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Rhode Island, and Puerto Rico residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/, 1-888-743-0023.

New Mexico residents: New Mexico consumers have the right to obtain a security freeze or submit a declaration of removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;

(2) proper identification to verify your identity; and

(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone. A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act. If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For New York residents: You may contact the New York Attorney General at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/. Additional information is available at the New York Department of State Division of Consumer Protection website, https://ag.ny.gov/consumer-frauds-bureau/identity-theft.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226 or 1-919-716-6000.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1-401-274-4400. You have the right to file or obtain a police report. You have the right to request a security freeze as described above.

For South Carolina residents: You may contact the South Carolina Department of Consumer Affairs at 1-800-922-1594 for guidance on preventing and minimizing the effects of identity theft.

For District of Columbia residents: You may contact the Office of Attorney General for the District of Columbia, Office of Consumer Protection, 400 6th Street NW, Washington, DC 20001; https://oag.dc.gov/; 1-202-727-3400 or 1-202-442-9828.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.