Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut



SparkMD Inc
Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Dear Parent or Guardian of <<Var data 1/Children's Names>>:

On behalf of <<Data Owner Entity PC Name>> ("Blueberry Medical"), I am writing to inform you of a security incident that affected limited elements of your children's protected health information ("PHI"). On August 22, 2026, Blueberry Medical discovered evidence of a data security issue that was created by a criminal exploitation of a vulnerability at Metabase, one of Blueberry Medical's technology providers, which resulted in the theft of a copy of some Blueberry Medical patient data. Because Metabase provides services to many companies (not just Blueberry Medical), you may receive more than one notice based on the same exploit that maps back to the Metabase vulnerability.

What Information Was Involved?
The information that may have been exposed to the unknown actor could include: name, health plan name and policy number, date of birth, and health care information such as medical records, dates of service, medical codes, and charges for services. Importantly, the photos and medically necessary videos that aid clinicians in rendering a diagnosis are stored separately, are secure, and were not compromised. **To confirm, the information did not include Social Security Numbers or payment information**.

What Happened?
Metabase is a third-party technology tool used by more than 100,000 organizations. Blueberry Medical uses Metabase for business intelligence needs such as reporting and data analysis. In August, Metabase disclosed that its software contained a previously unknown security vulnerability that could allow an unauthorized actor to gain access to customer instances and data. The exploitation of that vulnerability resulted in unauthorized access to Blueberry Medical's Metabase environment and the theft of a copy of certain patient data. Within hours of learning of the incident, Blueberry Medical locked an unauthorized party out of its system, hardened its system using the patch subsequently distributed by Metabase, and changed the appropriate passwords and security protocols. Blueberry Medical also reached out to law enforcement and retained a leading forensic and cyber security response firm.

What We Are Doing?
To prevent future occurrences and in light of the Metabase incident, Blueberry Medical has strengthened its authentication, implemented an additional monitoring and escalation process for its vendors' critical vulnerabilities, and increased the frequency of security reviews for third-party and self-hosted technology infrastructure, such as Metabase.

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

What Can You Do?

We emphasize that Blueberry Medical takes this matter very seriously and protecting the privacy and security of the PHI entrusted to us is extremely important to us. We apologize for any inconvenience that this event may cause. Although this incident did not involve certain sensitive financial information that would increase the risk of identity theft, we are providing the following information to you out of an abundance of caution. We still recommend that you remain vigilant by reviewing account statements and monitoring free credit reports, which are available via the sources below.

- **Review Accounts and Credit Reports:** You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

- You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protecting against identity theft. The FTC can be reached at: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

  For Iowa Residents: You may report suspected incidents of identity theft to local law enforcement or contact the Iowa Office of the Attorney General: Iowa Office of the Attorney General, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa, 50319, 515-281-6771, https://www.iowaattorneygeneral.gov/for-consumers/.

  For Maryland Residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

  For New York Residents: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/internet/privacy-and-identity-theft.

  For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

  For Oregon Residents: You may also report suspected identity theft to local law enforcement, including the Oregon Office of the Attorney General: Oregon Office of the Attorney General, Consumer Protection, 1162 Court St. NE, Salem, OR 97301, 1-877-877-9392, https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/data-breaches/.

  For Rhode Island Residents: By law, you have a right to obtain a police report filed relating to these incidents (if any), and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

For Washington, D.C. Residents: You may also obtain information about preventing and avoiding identity theft from the Washington D.C. Attorney General's Office: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001, (202) 727-3400, https://oag.dc.gov/consumerprotection.

- **Security Freezes and Fraud Alerts:** 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 at no charge. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

  A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

  As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed below.

  You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the following national credit reporting agencies:

National Credit Reporting Agencies Contact Information		
Equifax (www.equifax.com) **General Contact:** P.O. Box 740241, Atlanta, GA 30374 800-685-1111 **Fraud Alerts and Security Freezes:** P.O. Box 740256, Atlanta, GA 30374	Experian (www.experian.com) **General Contact:** P.O. Box 2104, Allen, TX 75013 888-397-3742 **Fraud Alerts and Security Freezes:** P.O. Box 9556, Allen, TX 75013	TransUnion (www.transunion.com) **General Contact, Fraud Alerts and Security Freezes:** P.O. Box 2000, Chester, PA 19022 800-916-8800

If you have any questions regarding this matter, please call us at 888-752-8498 Month through Friday, 9:00 AM to 9:00 PM, Eastern Time or email us at help@blueberrypediatrics.com.

Sincerely,

[Blueberry signatory]

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

SparkMD Inc
Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Re: Notice of Security Incident

Dear <<Full Name>>:

On behalf of <<Data Owner Entity PC Name>> ("Blueberry Medical"), I am writing to inform you of a security incident that affected limited elements of your protected health information ("PHI"). On August 22, 2026, Blueberry Medical discovered evidence of a data security issue that was created by a criminal exploitation of a vulnerability at Metabase, one of Blueberry Medical's technology providers, which resulted in the theft of a copy of some Blueberry Medical patient data. Because Metabase provides services to many companies (not just Blueberry Medical), you may receive more than one notice based on the same exploit that maps back to the Metabase vulnerability.

What Information Was Involved?
The information that may have been exposed to the unknown actor could include: name, health plan name and policy number, date of birth, and health care information such as medical records, dates of service, medical codes, and charges for services. Importantly, the photos and medically necessary videos that aid clinicians in rendering a diagnosis are stored separately, are secure, and were not compromised. **To confirm, the information did not include Social Security Numbers or payment information**.

What Happened?
Metabase is a third-party technology tool used by more than 100,000 organizations. Blueberry Medical uses Metabase for business intelligence needs such as reporting and data analysis. In August, Metabase disclosed that its software contained a previously unknown security vulnerability that could allow an unauthorized actor to gain access to customer instances and data. The exploitation of that vulnerability resulted in unauthorized access to Blueberry Medical's Metabase environment and the theft of a copy of certain patient data. Within hours of learning of the incident, Blueberry Medical locked an unauthorized party out of its system, hardened its system using the patch subsequently distributed by Metabase, and changed the appropriate passwords and security protocols. Blueberry Medical also reached out to law enforcement and retained a leading forensic and cyber security response firm.

What We Are Doing?
To prevent future occurrences and in light of the Metabase incident, Blueberry Medical has strengthened its authentication, implemented an additional monitoring and escalation process for its vendors' critical vulnerabilities, and increased the frequency of security reviews for third-party and self-hosted technology infrastructure, such as Metabase.

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

What Can You Do?

We emphasize that Blueberry Medical takes this matter very seriously and protecting the privacy and security of the PHI entrusted to us is extremely important to us. We apologize for any inconvenience that this event may cause. Although this incident did not involve certain sensitive financial information that would increase the risk of identity theft, we are providing the following information to you out of an abundance of caution. We still recommend that you remain vigilant by reviewing account statements and monitoring free credit reports, which are available via the sources below.

- **Review Accounts and Credit Reports:** You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

- You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protecting against identity theft. The FTC can be reached at: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

  For Iowa Residents: You may report suspected incidents of identity theft to local law enforcement or contact the Iowa Office of the Attorney General: Iowa Office of the Attorney General, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa, 50319, 515-281-6771, https://www.iowaattorneygeneral.gov/for-consumers/.

  For Maryland Residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

  For New York Residents: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/internet/privacy-and-identity-theft.

  For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

  For Oregon Residents: You may also report suspected identity theft to local law enforcement, including the Oregon Office of the Attorney General: Oregon Office of the Attorney General, Consumer Protection, 1162 Court St. NE, Salem, OR 97301, 1-877-877-9392, https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/data-breaches/.

  For Rhode Island Residents: By law, you have a right to obtain a police report filed relating to these incidents (if any), and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

For Washington, D.C. Residents: You may also obtain information about preventing and avoiding identity theft from the Washington D.C. Attorney General's Office: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001, (202) 727-3400, https://oag.dc.gov/consumerprotection.

- **Security Freezes and Fraud Alerts:** 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 at no charge. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

  A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

  As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed below.

  You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the following national credit reporting agencies:

National Credit Reporting Agencies Contact Information		
Equifax (www.equifax.com) **General Contact:** P.O. Box 740241, Atlanta, GA 30374 800-685-1111 **Fraud Alerts and Security Freezes:** P.O. Box 740256, Atlanta, GA 30374	Experian (www.experian.com) **General Contact:** P.O. Box 2104, Allen, TX 75013 888-397-3742 **Fraud Alerts and Security Freezes:** P.O. Box 9556, Allen, TX 75013	TransUnion (www.transunion.com) **General Contact, Fraud Alerts and Security Freezes:** P.O. Box 2000, Chester, PA 19022 800-916-8800

If you have any questions regarding this matter, please call us at 888-752-8498 Month through Friday, 9:00 AM to 9:00 PM, Eastern Time or email us at help@blueberrypediatrics.com.

Sincerely,

[Blueberry signatory]