424 Savannah Road, Lewes DE, 19958
beebehealthcare.org | (302) 645-3300

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

RE: NOTICE OF DATA BREACH
Important Security Notification. Please read this entire letter.

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Beebe Medical Center is writing to inform you of a data security incident experienced by Blackbaud, Inc. ("Blackbaud"), a provider of cloud-based database management services to Beebe, as well as many other not-for-profit organizations, schools, colleges and medical centers worldwide.

We take the privacy and security of all information very seriously. While we have no evidence to suggest that any of the impacted information was viewed or misused during this compromise, it is crucial that we be as supportive and transparent as possible. That is why we are writing to inform you of this incident and offer information about steps that can be taken to help protect your information.

What Happened:

On July 16, 2020, we were were notified by Blackbaud that it had discovered and stopped a ransomware attack that occurred between February 7, 2020 and May 20, 2020. Blackbaud's systems that were affected by the attack included a database containing certain data related to Blackbaud clients. At this time, Blackbaud's communications indicated that Beebe data was not impacted. Thereafter, in November 2020, Blackbaud provided additional notification that Beebe data was in fact contained within the impacted database. According to the notification provided by Blackbaud, the attacker(s) may have acquired an unknown amount of data maintained within Blackbaud's database. Blackbaud informed us that it paid a demand to the attacker and obtained confirmation that the compromised information had been destroyed and is no longer in the possession of the attacker(s). According to Blackbaud, and as far as we know, there is no indication that any of the compromised information has been subject to misuse or to further disclosure. Nevertheless, out of an abundance of caution, we wanted to advise you of this incident and provide you with resources to protect your personal information.

Blackbaud's November notification contained minimal information regarding the scope of impacted information as it relates to Beebe and our community. Upon discovery, we immediately undertook an in-depth investigation, with the assistance of independent forensic experts, into the impacted data. Due to the complex nature of the data provided by Blackbaud, this process took significant time.

What Information Was Involved:

Upon receipt of Blackbaud's notification, Beebe immediately began an internal investigation to determine the scope of the incident reported by Blackbaud. This included obtaining a copy of the impacted data from Blackbaud for further investigation. On December 2, 2020, after significant review, Beebe discovered that your personal information may have been contained within the affected Blackbaud database. Based on Beebe's investigation, the information potentially impacted as a result of the incident experienced by Blackbaud includes your name in combination with one or more of the following data elements: date of birth; Clinician name; date of screening; visit date; and department related to medical services. Importantly, no Social Security numbers or financial account numbers were impacted as a result of this incident.

What Is Being Done:

Blackbaud has indicated that they are taking efforts to further secure their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms. Additionally, Blackbaud has stated that they are working to expand their use of encryption technologies to further secure all data within the Blackbaud environment.

What You Can Do:

We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. We have provided additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information:

Should you have questions or concerns regarding this matter, please do not hesitate to contact 1-833-971-3295, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. The security of our community's personal information is of the utmost importance to us and we deeply regret this incident.

We stay committed to protecting your trust in us and continue to be thankful for your support of Beebe Medical Center. Please accept our regret for any worry or inconvenience that this Blackbaud incident may cause you.

Sincerely,

Jacqueline Emory
Chief Compliance Officer

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

PLACE A 1-YEAR FRAUD ALERT ON YOUR CREDIT FILE

An initial 1-year security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request when a fraud alert is active. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

TransUnion	**Experian**	**Equifax**
Fraud Victim Assistance Dept.	National Consumer Assistance	Consumer Fraud Division
P.O. Box 6790	P.O. Box 1017	P.O. Box 105069
Fullerton, CA 92834	Allen, TX 75013	Atlanta, GA 30348
1-800-680-8289	1-888-397-3742	1-800-525-6285
www.transunion.com	www.experian.com	www.equifax.com

PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with any new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting agencies. 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. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. In order to request a security freeze,you will need to provide some or all of the following informationto the credit reporting agency, depending on whether you do so online, by phone, or by mail: 1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.); 2. Social Security Number; 3. Date of birth; 4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years; 5. Proof of current address,suchas a current utility bill, telephone bill, rental agreement, or deed; 6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); 7. Social Security Card, pay stub, or W2; 8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

ORDER YOUR FREE ANNUAL CREDIT REPORTS

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. Visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with; and shredding receipts, statements, and other sensitive information. Remain vigilant by reviewing account statements and monitoring credit reports.

USE TOOLS FROM CREDIT PROVIDERS

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

BE AWARE OF SUSPICIOUS ACTIVITY INVOLVING YOUR HEALTH INSURANCE

Contact your healthcare provider if bills do not arrive when expected, and review your Explanation of Benefit forms to check for irregularities or suspicious activity. You can also contact your health insurance company to notify them of possible medical identity theft or ask for a new account number.

RIGHTS UNDER THE FAIR CREDIT REPORTING ACT (FCRA)

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

OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. Additionally, any suspected identity theft should be reported to law enforcement, including your state Attorney General and the Federal Trade Commission. Additional information is available at http://www.annualcreditreport.com. Under Rhode Island and Massachusetts law, you have the right to obtain any police report filed in regard to this incident.

- Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity.
- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft. For Mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, DC 20580.
- **For Maryland residents,** the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.
- **For New York residents,** 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/consumerprotectionl; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov
- **For North Carolina residents,** the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.
- **For Rhode Island Residents,** the Attorney General can be contacted at 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov or 401-274-4400.