NOTICE OF DATA INCIDENT

ABOUT THE DATA PRIVACY EVENT

Jewish Home Lifecare d/b/a The New Jewish Home is providing notice of an incident at one of its third-party vendors that may affect the privacy of some information relating to certain individuals associated with The New Jewish Home.

FREQUENTLY ASKED QUESTIONS

What Happened?

On Thursday, July 16, 2020, The New Jewish Home was among many organizations across the country notified that one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), was the target of a cyber incident. Blackbaud is one of the most commonly utilized cloud computing providers that offers customer relationship management and financial services tools for many independent schools, universities, and non-profit organizations. The New Jewish Home itself was not the target of this incident and did not experience any internal breach of data including medical records, which remain secure. The New Jewish Home is the parent organization of The New Jewish Home, Manhattan; The New Jewish Home, Sarah Neuman; The New Jewish Home, Home Care; The New Jewish Home, University Avenue Assisted Living; Jewish Home Lifecare, Home Assistance Personnel, Inc.; The New Jewish Home, Corporate Services, as well as The Fund for the Aged (collectively, "The New Jewish Home"). The Fund for the Aged is the entity that uses the Blackbaud software in order to coordinate fundraising for The New Jewish Home.

Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. Unfortunately, Blackbaud's incident impacted a significant number of these organizations, including The New Jewish Home.

Blackbaud has provided the following link for additional information on this incident: https://www.blackbaud.com/securityincident.

Upon learning of the Blackbaud incident, The New Jewish Home immediately commenced an investigation to determine what, if any, sensitive The New Jewish Home data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. On August 14, 2020, The New Jewish Home received further information from Blackbaud that allowed it to confirm that the information potentially affected may have contained health care related information for some The New Jewish Home patients and former patients.

What Information Was Involved? The information maintained by Blackbaud includes individuals' name, address, date of birth, date of death, and bank account information. Social

Security numbers were impacted only for a small percentage of the impacted population. According to Blackbaud, based on the nature of the incident, their research, and third-party (including law enforcement) investigation, they have no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise be made available publicly.

What is The New Jewish Home Doing? The New Jewish Home takes the security of information entrusted to it very seriously and apologizes for the inconvenience this incident has caused. As part of its ongoing commitment to the security of information in its care, The New Jewish Home is working to review its existing policies and procedures regarding its third-party vendors, and is working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. The New Jewish Home is also notifying state and federal regulators, where required. Blackbaud has advised The New Jewish Home that the data potentially obtained by the attacker through this event was destroyed and that they have implemented additional security measures.

What Can Impacted Individuals Do? As a best practice, The New Jewish Home encourages individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, explanation of benefits, and credit reports for suspicious activity. Individuals may also review the information contained in the attached *Privacy Safeguards*.

For More Information? Impacted individuals may write to The New Jewish Home at 120 West 106th Street, New York, NY 10025 or call The New Jewish Home's dedicated assistance line at (212) 870-5041 with questions.

PRIVACY SAFEGUARDS

Monitor Your Accounts

Potentially affected individuals may also consider the information and resources outlined below.

The New Jewish Home encourages affected individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the 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. 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. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze	PO Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/credit-report-services

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

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, provide the addresses where you have 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 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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services

Additional Information

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.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from 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 www.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.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Rhode Island Residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

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