Notice of Limited Social Engineering Cybersecurity Incident

October 16, 2026

In August 2026, we experienced a limited social engineering cybersecurity incident that did not impact our operations, and did not involve our Electronic Health Records platform. As described below, the incident involved access to certain files used for general nonprofit governance purposes, which can include summaries primarily related to patient care costs. We are carefully reviewing those files to identify what patient information is involved and to whom it relates. We will provide direct notice to patients after the review is complete. In the meantime, we are sharing this notice to keep patients informed and to provide optional precautionary steps.

What Happened? Between August 3 and 4, 2026, a user account was accessed after a phishing incident. During that time, an unauthorized individual accessed the user account and copied files. The files were generally nonprofit governance materials, including financial and budgeting information, administration records, and presentations. However, within the budgeting information there may be high level summaries related to patient care costs. The files are undergoing detailed review in order to catalogue which patients may have information involved in order for us to notify those patients directly.

What Information Was Involved? As referenced above, this matter did not involve our Electronic Health Records platform. The types of information that may be involved, which are subject to change, include demographic information and patient identifiers such as name, address, other contact information, and/or date of birth. With respect to health and health payment related services, this can include demographic information and medical record number, patient account number, treatment types, dates and care costs.

What We Are Doing. We have robust cyber governance training and monitoring practices. As part of our response to this matter, we are evaluating our staff training and account activity monitoring procedures to identify areas for improvement. We are also reporting this incident to the U.S. Department of Health and Human Services.

What Individuals Can Do. Based on the files reviewed to date, the information identified is limited and generally does not include enough identifying information, on its own, to identify individual patients or facilitate identity theft or fraud. Our review remains ongoing, and we are continuing to determine whether any files contain more detailed patient identifiers. As a precaution, we have included free resources and practical guidance below for patients and parents or guardians who may wish to take additional steps. These optional steps include reviewing relevant account statements, obtaining free credit reports, and checking for unfamiliar activity or errors. Additional information about credit monitoring, fraud alerts, security freezes, and resources for protecting personal information appears in the sections below.

For More Information. If individuals have questions about this matter, we have an assistance line with agents ready to help answer those questions. You may contact our toll-free assistance line at 1-833-918-8844, Monday through Friday, from 8:00 a.m. to 8:00 p.m. Eastern Time (excluding U.S. holidays).

Thank you for your patience and understanding.

Sincerely,

Beth Israel Lahey Health, Inc.

STEPS INDIVIDUALS CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Relevant Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax—www.equifax.com; 1-888-298-0045; and P.O. Box 105788 Atlanta, GA 30348-5788
Experian—www.experian.com; 1-888-397-3742; and P.O. Box 9554, Allen, TX 75013
TransUnion—www.transunion.com; 1-833-799-5355; and P.O. Box 160, Woodlyn, PA 19094

For loved ones that may have recently passed, individuals may also place a "deceased – do not issue credit" flag on the loved one's credit file. Only one consumer reporting bureau needs to be notified, and it will notify the other two major consumer reporting bureaus. Individuals may complete this process using the information provided by the credit bureaus at the below websites:

Equifax: https://www.equifax.com/personal/help/article-list/-/h/a/relative-death-contact-credit-bureaus
Experian: https://www.experian.com/blogs/ask-experian/reporting-death-of-relative/
TransUnion: https://www.transunion.com/blog/credit-advice/reporting-a-death-to-tu

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their 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, 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. 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 they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are no known impacted Rhode Island residents as of this publication.

STEPS INDIVIDUALS CAN TAKE TO PROTECT THEIR MINOR DEPENDENTS' PERSONAL INFORMATION

Monitor Relevant Accounts

Typically, credit reporting agencies do not have a credit report in a minor's name. To find out if your minor dependent has a credit report or to request a manual search for your minor dependent's Social Security number, each credit bureau has its own process. To learn more about these processes or request these services, you may contact the credit bureaus by phone or in writing or you may visit or contact the below credit bureaus.

Equifax: https://www.equifax.com/personal/education/identity-theft/articles/-/learn/child-identity-theft/; 1-888-298-0045; and P.O. Box 105788 Atlanta, GA 30348-5788
Experian: https://www.experian.com/help/minor-request.html; 1-888-397-3742; and P.O. Box 9554, Allen, TX 75013
TransUnion: https://www.transunion.com/fraud-victim-resources; 1-833-799-5355; and P.O. Box 160, Woodlyn, PA 19094

To request information about the existence of a credit file in your minor dependent's name, search for your dependent's Social Security number, place a security freeze on your dependent's credit file, place a fraud alert on your dependent's credit report (if one exists), or request a copy of your dependent's credit report you may be required to provide some or all the following information:

- A copy of your driver's license or another government issued identification card, such as a state identification card, etc.;
- Proof of your address, such as a copy of a bank statement, utility bill, insurance statement, etc.;
- A copy of your minor dependent's birth certificate;
- A copy of your minor dependent's Social Security card;
- Your minor dependent's full name, including middle initial and generation, such as JR, SR, II, III, etc.;
- Your minor dependent's date of birth; and
- Your minor dependent's previous addresses for the past two years.

Additional Information

Individuals may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps individuals can take to protect 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, 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. Individuals can obtain further information on how to file such a complaint by way of the contact information listed above. Individuals and/or their minor dependent have the right to file a police report if their minor dependent ever experiences identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, individuals or their minor dependent will likely need to provide some proof that their minor dependent has been a victim. Instances of known or suspected identity theft should also be reported to law enforcement.