Notice of Data Security Incident

April 10, 2026

Notice of Data Security Incident

The privacy and security of the personal information entrusted to us is of the utmost importance to Springfield Hospital. We are writing to provide you with information regarding a recent cybersecurity incident. As such, we wanted to provide you with information about the incident, explain the services we are making available to impacted patients, and let you know that we continue to take significant measures to protect personal and protected health information.

Springfield Hospital recently discovered that one employee email account was accessed by an unauthorized actor on December 17, 2025. Upon learning of this issue, Springfield Hospital immediately took steps to secure our email tenant and commenced a prompt and thorough investigation. The investigation aimed to determine the nature and scope of the incident and whether any sensitive data, including personal and/or health information, was accessed and/or acquired by the unauthorized party.

Following this investigation, we learned on February 10, 2026, that the impacted email account that was accessed on December 17, 2025, contained a limited amount of personal and health information that may have been accessed by the unauthorized party. The data involved in the incident contained the personal information of certain individuals, including full name in combination with one or more of the following: date of birth, Social Security number, reason for visit, treating physician name, and medical record number. Please note that impacted information varies by individual.

We have no evidence that any information has been misused as a direct result of this incident. Nevertheless, out of an abundance of caution, we are notifying affected individuals of the scope of the incident. This notice includes precautionary measures individuals can take to protect their personal information, including placing a Fraud Alert and Security Freeze on your credit files and obtaining a free credit report. Additionally, impacted individuals should always remain vigilant in reviewing their credit reports on a regular basis and report any irregular activity immediately.

Please accept our apologies that this incident occurred. Springfield Hospital remains fully committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it, including continually evaluating and modifying its practices and internal controls.

Individuals who think they may have been impacted and did not receive a notification letter, or have any further questions regarding this incident can call our dedicated and confidential toll-free response line that we have to set up to respond to questions at 833-289-6183.

This response line is staffed with professionals familiar with this incident and knowledgeable on what can be done to protect personal information. The response line is available Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time, excluding holidays.

Springfield Hospital

25 Ridgewood Road

PO Box 2003

Springfield, VT 05156

– OTHER IMPORTANT INFORMATION –

1. Obtain and Monitor Your Credit Report

Under federal law, you are entitled to one free credit report every 12 months from each of the three major nationwide credit reporting companies. You can obtain a free copy of your credit report by calling **1-877-322-8228,** visiting **http://www.annualcreditreport.com,** or by

completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/index.action. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below.

Equifax P.O. Box 105069 Atlanta, GA 30348-5069 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (800) 525-6285	***Experian*** P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html (888) 397-3742	***TransUnion*** Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016-2000 https://www.transunion.com/fraud-alerts (800) 680-7289

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.

2. Placing a Fraud Alert on Your Credit File.

You can place an initial 1-year "fraud alert" on your credit files, at no charge. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others. Additional information is available at https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/.

Equifax P.O. Box 105069 Atlanta, GA 30348-5069 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (800) 525-6285	***Experian*** P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html (888) 397-3742	***TransUnion*** Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016-2000 https://www.transunion.com/fraud-alerts (800) 680-7289

3. Placing a Security Freeze on Your Credit File.

Following is general information about how to request a security freeze from the three credit reporting agencies at no charge. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided below). You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348-5788 https://www.equifax.com/personal/credit-report-services/credit-freeze/ (888)-298-0045	***Experian Security Freeze*** P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze (888) 397-3742	***TransUnion Security Freeze*** P.O. Box 160 Woodlyn, PA 19094 https://www.transunion.com/credit-freeze (888) 909-8872

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

4. Protecting Your Medical Information.

We have no evidence that your medical information involved in this incident was or will be used for any unintended purposes. However, the following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at http://www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina,

Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, http://www.doj.state.or.us/, Telephone: 877-877-9392.

37802763.1