In December of 2024, HCRS experienced a data security incident when an unauthorized individual gained access to two staff email accounts. If your information was affected, you will receive a letter from us soon with details about this incident and steps you can take to best protect yourself.

If you have any questions or need support, please reach out to Rose Nevins-Alderfer at rnevins@hcrs.org. We're here to help.

Health Care and Rehabilitation Services of Southeastern Vermont, Inc. ("HCRS")
Notice of Data Security Incident

Updated: June 9, 2025

Health Care and Rehabilitation Services of Southeastern Vermont, Inc. ("HCRS") is committed to protecting the privacy and security of the personal information we maintain. We are making individuals aware of a data security incident involving unauthorized access to two email accounts within our email environment. We immediately conducted an investigation into the incident and reset passwords to the affected accounts. As part of the investigation, we engaged third-party cybersecurity professionals experienced in handling these types of incidents. The investigation determined a limited number of individuals were affected by this incident. Although we have no evidence of financial or medical fraud or identity theft related to this incident, we are making potentially affected individuals aware of the incident, the resources we are making available to those affected, and steps that impacted individuals can take to best protect their personal information, should they feel it appropriate to do so.

What Happened? On December 20, 2024, HCRS identified unauthorized access to two email accounts in its email environment. Upon detecting the unauthorized activity, HCRS immediately worked to contain the incident and launched a thorough investigation into the matter. As a part of the investigation, HCRS engaged leading outside cybersecurity professionals to secure the email environment and to identify the scope of what personal information, if any, was involved. After an extensive forensic investigation and complex third-party manual review, HCRS discovered on May 13, 2025, that certain email accounts within the HCRS email environment were accessed by an unauthorized actor between approximately December 4, 2024, to on or about December 9, 2024. The investigation determined the emails and files accessed by the unauthorized party contained certain personal information for clients and staff. To date, we have no evidence of financial fraud or identity theft related to the impacted information. Nevertheless, we will be providing notice of the incident to the individuals whose personal information was potentially impacted.

What Information Was Involved? The information involved includes first and last names, dates of birth, Social Security numbers, financial account numbers, dates of treatment or service, individual health insurance information, medical history, driver's license numbers, patient numbers, MRNs, healthcare billing information, and other medical treatment information. The types of impacted information varied by individual.

What We Are Doing. The security and privacy of the information we maintain is a top priority for us. In response to this incident, we took immediate steps to secure our email environment and engaged third-party forensic experts to assist in the investigation. HCRS continually evaluates and modifies its practices and internal controls to enhance the security and privacy of individual personal information and will continue to do so in light of this incident.

How will Individuals Know if They are Affected by this Incident? HCRS is providing notice to individuals whose information was determined to be contained in the impacted email accounts, in accordance with our legal obligations and to the extent we have valid mailing addresses for the individuals. If an individual does not receive a letter but would like to know if they are potentially affected, they may contact Rosie Nevins-Alderfer at rnevins@hcrs.org.

For More Information. **If you have any questions regarding this incident, we are in the process of setting up a dedicated and confidential toll-free response line and will update that information within a few days.** This response line will be staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against potential misuse of your information. The response line will be available 8:00am to 8:00pm ET, Monday through Friday, excluding holidays.

What You Can Do. We encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits forms, and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report, place a fraud alert, or a security freeze. Contact information for the credit bureaus is below:

— OTHER IMPORTANT INFORMATION—

1. Placing a Fraud Alert on Your Credit File.

You may place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. 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.

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

2. **Consider Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. 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'll 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.

If you do place a security freeze *prior* to enrolling in any credit monitoring service, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

3. **Additional Information**

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your 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. 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.

4. **<u>Protecting Your Medical Information</u>.**

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.

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.

* * *