WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

September 26, 2025

Joseph Fusz
(312) 821-6141
Joseph.Fusz@WilsonElser.com

Via Online Portal:

Attorney General Nick Brown
1125 Washington St SE
PO Box 40100
Olympia, WA 98504

Re: Cybersecurity Event Involving Emergency Responders Health Center

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Emergency Responders Health Center ("ERHC"), located at 9976 West Emerald, Boise, ID 83704, with respect to a recent cybersecurity event (the "Event") that ERHC first became aware of on April 11, 2025. ERHC takes the security and privacy of the information in its control very seriously and has taken steps to mitigate against the risk of a similar event occurring in the future.

This letter will serve to inform you of the nature of the Event, the notifications provided to individuals potentially affected by the Event, and the steps that ERHC has taken in response to the Event. By providing this notice, ERHC does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

1. Nature of the Event

On April 11, 2025, ERHC became aware of suspicious activity in one of its email accounts. Upon becoming aware, ERHC immediately secured the account and promptly engaged third-party cybersecurity specialists to conduct a comprehensive forensic investigation into the nature and scope of the Event. Through the investigation, it was determined that certain ERHC email accounts may have been compromised by an unauthorized actor. The accounts have all since been secured and remediated. Based on these findings, ERHC performed an extensive and detailed review of the impacted accounts to identify the types of information present and to catalog any identifiable individuals to whom such information related. On September 16, 2025, ERHC finalized the list of individuals to notify.

2. Washington Residents Affected

ERHC identified 1,528 total individuals potentially affected by this Event. Of those, five hundred and twenty-six (526) are Washington residents. The information relating to Washington residents

that may have been impacted varies by individual but includes names, dates of birth, Driver's License numbers, Social Security Numbers, medical information, and health insurance information. Notification letters were mailed on September 26, 2025. A sample copy of the notification letter was uploaded via the online Data Breach Notification Form.

3. **Steps Taken in Response to the Event.**

ERHC treats this Event with the utmost seriousness and the privacy, security, and confidentiality of information in ERHC's care are among its highest priorities. Upon becoming aware of the Event, ERHC moved promptly to respond including by securing and remediating the affected accounts, engaging digital forensic specialists to investigate the Event, and performing an exhaustive review of the at-risk data in order to notify potentially affected individuals. Furthermore, ERHC is taking steps to prevent a similar event from occurring in the future by implementing additional technical safeguards, enhanced security measures, and updated policies and procedures. Finally, ERHC is providing notified individuals complimentary offers for twelve (12) months of credit monitoring and identity theft restoration services.

4. **Contact information**

ERHC remains dedicated to protecting the information in its control. Should you have any questions or need additional information, you can contact me at Joseph.Fusz@wilsonelser.com or 312-821-6141.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Joseph Fusz, Esq.

Emergency Responders Health Center
PO Box 5012
Branchburg NJ 08876

0000001**000001*****ALL FOR AADC 990*****000001**000001

0000001

[redacted]

September 26, 2025

Re: Notice of Data Security Event

Dear [redacted],

Emergency Responders Health Center ("ERHC") writes to inform you of a recent cybersecurity event that may have impacted the security of your personal information. While we are unaware of any misuse of your personal information at this time, we are providing you with details about the event, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened?

On April 11, 2025, we detected unusual activity on one of our email accounts. Upon becoming aware of this, we immediately secured the account and promptly engaged a specialized third-party cybersecurity firm to conduct a comprehensive forensic investigation into the nature and scope of the issue. The forensic investigation determined that several ERHC email accounts may have been compromised by an unauthorized actor between December 11, 2024 and April 11, 2025. The accounts have since been secured.

Based on these findings, we reviewed the affected accounts to identify the specific individuals and the types of information that may have been at-risk. On September 16, 2025, we finalized the list of individuals to notify.

What Information Was Involved?

Although we have no evidence that any sensitive information has been misused by third parties as a result of this event, we are notifying you out of an abundance of caution and for purposes of full transparency. Our review found that your name and the following personal information relating to you were present within data potentially at risk: [redacted].

What We Are Doing.

ERHC takes this event seriously and the privacy, security, and confidentiality of information in our care are among our highest priorities. Upon becoming aware of the event, we moved quickly to promptly investigate and respond to the event. Specifically, we took steps to secure our systems and are implementing additional technical safeguards and enhanced security measures to mitigate against the risk of future issues. We are notifying potentially affected individuals, including you, so that you may take further steps to best protect your information, should you feel it is necessary to do so.

We are also providing you with 12 months of complimentary credit monitoring, fraud consultation, and identity theft restoration services through HaystackID. While ERHC is covering the cost of these services, you will need to complete the activation process yourself by following the instructions below.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, to monitor your credit reports for suspicious or unauthorized activity, and to report any suspicious activity promptly to your

bank, credit card company, or other applicable institution. Please review the enclosed *Additional Resources to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse. Furthermore, you may also activate the credit monitoring services, according to the instructions provided below, which we are making available to you at no cost.

Credit Monitoring Enrollment Instructions

To enroll in the free credit monitoring services noted above, please log on to https://app.identitydefense.com/enrollment/activate/ERHC and follow the instructions provided. When prompted, please [redacted]. In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. Enrollment requires an internet connection and e-mail address and may not be available to minors under the age of eighteen (18) years of age. Please note that, when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information.

If you have any questions or concerns not addressed in this letter, please call 800-695-7289 (toll free) during the hours of 8:00 am to 11:00 pm Eastern time, Monday through Friday and 9:00 am to 6:00 pm Saturday (excluding U.S. national holidays).

Sincerely,

Emergency Responders Health Center

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity. You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies. You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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 should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 www.equifax.com/personal/credit-report-services
TransUnion	P.O. Box 1000 Chester, PA 19016 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx. Emergency Responders Health Center is located at 9976 West Emerald, Boise, ID 83704.

New York residents are advised that in response to this event they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this event and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.