

Hudson Valley Medical Billing & Credentialing, LLC
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

<FirstName> <LastName>
<Address1>
<Address2>
<<City>>, <<State>> <<PostalCode+4>>

July 7, 2026

Dear <<FirstName>> <<LastName>>,

Hudson Valley Medical Billing & Credentialing, LLC ("HVMBC") provides patient billing and accounts receivable services to <<Custom Field 2>>. We are writing to notify you of an incident that may have involved some of your health information. We have no evidence that your information has been misused and sincerely apologize for any concern or inconvenience this may cause you. This letter explains the incident and what we are doing in response. It also contains information about steps you can take to protect your information and resources we are making available to help you.

What Happened? On March 6, 2026, HVMBC became aware of possible unauthorized access to a computer system. Immediately after learning of the potential unauthorized access, the affected computer was shut down, and an investigation was initiated to determine whether any health information was impacted. We were unable to determine whether any specific materials on our system were accessed during the possible incident. However, because health information was present on the system and may have been accessible, we are providing this notice out of an abundance of caution.

What Information Was Involved? The information may include some combination of your name, <<Exposed Data Elements>>.

What We Are Doing: We want to assure you that we are taking steps to minimize the risk of this happening again in the future. Since the incident, we have worked to restore our systems, tighten access controls, and are evaluating additional technical safeguards to strengthen the security of our systems. In addition, although there has been no evidence that your information was misused, we are offering you credit monitoring and identity protection services through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services for <<Service Length>> at no charge. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

What You Can Do: You should remain vigilant in reviewing your financial account statements and credit reports over the next 12 to 24 months and notify your financial institution if you become aware of fraudulent or irregular activity. Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. We also encourage you to take full advantage of the service offering through Cyberscout. To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted, please provide the following unique code to receive services: <<UniqueCode>>. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 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 questions, please call 1-833-851-4874 Monday through Friday from 8:00 am–8:00 pm Eastern Time, excluding holidays. Protecting your information is important to us, and we sincerely apologize for any concern this incident may cause you.

Sincerely,

Ilene Kaswer, President

Hudson Valley Medical Billing & Credentialing, LLC

Recommended Steps to Help Protect Your Information

1. Website and Enrollment. You can enroll in the complimentary credit monitoring services being offered to you by logging on to <https://bfs.cyberscout.com/activate> and following the provided instructions. When prompted, please provide the unique code provided in this letter. The enrollment requires an internet connection and email account and may not be available to minors. 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.

2. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

3. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-800-525-6285
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19016
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

4. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 a 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. You can 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.

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/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. 0 Rhode Island residents were notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.