Centers for Medicare & Medicaid Services
7500 Security Blvd.
Baltimore, MD 21244-1850

Name
Address
City, State ZIP

December 16, 2022

Dear <Name>,

We are writing to inform you of a potential privacy incident involving your personal information related to Medicare entitlement and premium payment records. The Centers for Medicare & Medicaid Services (CMS), the federal agency that manages the Medicare program, is sending you this letter so that you can understand more about this incident, how we are addressing it, and additional steps you can take to protect your privacy. We will issue you a new Medicare card with a new Medicare Number and have provided information with this notice on free credit monitoring services. This does not impact your Medicare benefits or coverage.

What Happened?

On October 8, 2022, Healthcare Management Solutions (HMS), LLC, a CMS subcontractor, was subject to a ransomware attack on its corporate network. HMS handles CMS data as part of processing Medicare eligibility and entitlement records, in addition to premium payments. Initial information indicates that HMS acted in violation of its obligations to CMS, and CMS continues to investigate the incident. No CMS systems were breached, and no Medicare claims data were involved. On October 9, 2022, CMS was notified that the subcontractor's systems had been subject to a cybersecurity incident but CMS systems were not involved. As more information became available, on October 18, 2022, CMS determined with high confidence that the incident potentially included personally identifiable information and protected health information for some Medicare enrollees. Since then, CMS has been working diligently with the contractor to determine what information and which individuals may have been impacted.

What Information Was Involved?

After careful review, we have determined that your personal and Medicare information may have been compromised. This information may have included the following:

- Name
- Address
- Date of Birth
- Phone Number
- Social Security Number
- Medicare Beneficiary Identifier
- Banking information, including routing and account numbers
- Medicare Entitlement, Enrollment, and Premium Information.

No claims data were involved in this incident.

What We Are Doing

When the incident was reported, we immediately started an investigation, working with the contractor and cybersecurity experts to identify what personal information, if any, might have been compromised. CMS is continuing to investigate this incident and will continue to take all appropriate actions to safeguard the information entrusted to CMS.

What You Can Do

At this time, we're not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. However, out of an abundance of caution we are issuing you a new Medicare card with a new number. CMS will mail the new card to your address in the coming weeks. In the meantime, you can continue to use your existing Medicare card. After you get your new card, you should:

1. Follow the instructions in the letter that comes with your new card.
2. Destroy your old Medicare card.
3. Inform your providers that you have a new Medicare Number.

While we continue to investigate what, if any, banking information may have been compromised, if you have concerns, please contact your financial institution and let them know your banking information may have been compromised. Additionally, you can enroll in free Equifax Complete Premier credit monitoring service. You do **not** need to use your credit card to enroll in the service. To activate your free credit monitoring:

- Please review the attached insert with instructions
- You can enroll online or by calling xxx-xxx-xxxx
- **Enroll by March 31, 2023** Your code will not work after this date
- Visit the Equifax website to enroll at: **www.xxx.com**

For questions about the credit monitoring service or to enroll in Equifax Complete Premier over the phone, please call Equifax's customer care team by March 31, 2023 at xxx-xxx-xxxx.

We have enclosed additional information about other steps you can take to further protect your privacy.

For More Information

We take the privacy and security of your personal information very seriously. We apologize for the inconvenience this privacy incident has caused.

If you have any further questions regarding this incident, please call the Equifax dedicated and confidential toll-free response line at xxx-xxx-xxxx. This response line is staffed with professionals familiar with this incident who know what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9am to 9pm Eastern.

You can also call 1-800-MEDICARE (1-800-633-4227) with any general questions or concerns about Medicare.

Other Steps to Protect Yourself

1. Place a Fraud Alert on Your Credit File

The Federal Trade Commission (FTC) recommends that you 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 105788
Atlanta, GA 30348
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 LLC
P.O. Box 6790
Fullerton, PA 92834-6790
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 individually 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
https://www.equifax.com/personal/credit-report-services/credit-freeze/
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/creditfreeze
1-888-909-8872

To place the security freeze, you'll need to provide 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.

3. Obtain a Free 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 listed above. Call **1-877-322-8228** or request your free credit

reports online at **www.annualcreditreport.com**. When you receive your credit reports, review them for problems. Identify any accounts you didn't 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.

Even if you don't find any suspicious activity on your initial credit reports, the FTC recommends that you still 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 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.

4. Protect 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 don't 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. Follow up with your insurance company or the care provider for any items you don't recognize.

***IF YOU ARE A DISTRICT OF COLUMBIA RESIDENT**:* You may obtain information about avoiding identity theft from the FTC or the District of Columbia Attorney General's Office. These offices can be reached at:

Federal Trade Commission	Office of the Attorney General
Consumer Response Center	441 4th Street, NW
600 Pennsylvania Avenue, NW	Suite 1100 South
Washington, DC 20580	Washington, DC 20001
(877) IDTHEFT (438-4338)	(202) 727-3400
http://www.ftc.gov/idtheft/	https://oag.dc.gov/

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

IF YOU ARE A NEW YORK RESIDENT: You may obtain information about security breach response and identity theft prevention and protection from the FTC or from the following New York state agencies:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

New York Attorney General
Consumer Frauds &
Protection Bureau
120 Broadway, 3rd Floor
New York, NY 10271
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, New York 12231
(800) 697-1220
www.dos.ny.gov

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

North Carolina Department of Justice
Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.com

IF YOU ARE A RHODE ISLAND RESIDENT: You may contact state or local law enforcement to determine whether you can file or obtain a police report relating to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
http://www.riag.ri.gov/