United States Senate
WASHINGTON, DC 20510

May 20, 2026

The Honorable Mehmet Oz, M.D.
Administrator
Centers for Medicare and Medicaid Services
U.S. Department of Health and Human Services
7500 Security Boulevard
Baltimore, MD 21244

Dear Administrator Oz:

In our letter to you on November 4, 2025, we warned that the rushed deployment of the Center for Medicare & Medicaid Services' (CMS's) Medicare provider directory posed serious risks to the millions of seniors relying on it to make informed choices for plan selection during open enrollment. We asked who authorized the accelerated timeline, what testing was completed, and what accountability mechanisms existed. Your March 24, 2026 response, which arrived several months into open enrollment, did not address those questions. The year-long special enrollment period CMS is a necessary remedy to protect beneficiaries, but it is also a tacit admission that the underlying system was not ready for deployment.

We write again today with even greater concern. Reporting reveals that the provider directory exposed the Social Security numbers of health care providers, linked to their names and other personally identifiable information, on a public-facing federal website.[1] This same reporting identified dozens of affected providers in a sample of database rows. Critically, it appears CMS failed to detect this exposure for weeks and learned of it only when reporters made inquiries. This is precisely the category of data that bad actors have long used to perpetuate identity theft, and the harm to affected providers and to program integrity cannot be undone.

We view this as part of a broader and deeply troubling pattern. When we wrote to you in November 2025, we stressed that the rushed deployment of this provider directory led to the erroneous information included in the database. This administration has repeatedly mishandled sensitive personal data entrusted to the federal government and has repeatedly resisted congressional oversight when those failures come to light.

We therefore request written responses to the following questions no later than **June 3, 2026**:

The Incident: Timeline, Scope, and Notification

1. Provide a chronological account of the incident, including when CMS first became aware that provider Social Security numbers (SSNs) had been exposed in the directory database;

[1] "Trump administration inadvertently exposed Social Security numbers of health care providers in Medicare database," *The Washington Post*, Apr. 30, 2026, https://www.washingtonpost.com/health/2026/04/30/medicare-portal-social-security-numbers-exposed/

what actions were taken and at what times following that awareness; and which entities, including third-party contractors, were involved in said actions?

2. Have you identified the full extent of the exposure? Has the exposure been remediated? If yes, please provide the precise start and end dates of the exposure window.
3. How many providers' SSNs were exposed in total?
4. Please explain what purpose SSNs served in this database.
5. Besides SSNs, was any other personally identifiable information (PII) exposed? Please provide details.
6. Has CMS provided individual written notification to every provider whose PII was exposed in the database? If so, please provide the dates, means, and content of the notifications.
7. Has CMS conducted forensic analysis to determine whether unauthorized parties accessed, scraped, or exfiltrated the exposed data before the information was removed from the database? Provide details of the investigation, the entities involved, and any findings.

Accountability Frameworks

8. Please identify every political appointee—by name, title, and affiliation—who had decision-making authority over the design, development, database architecture, content, security, and deployment of the directory, or post-deployment maintenance.
9. Identify every individual affiliated with the Department of Government Efficiency (DOGE), or detailed to CMS from any DOGE-adjacent entity, who participated in any aspect of the directory's development, deployment, or post-deployment maintenance. Describe the nature of their access and authorities.
10. Identify every contractor and subcontractor involved in the directory, the procurement vehicle used for each, and whether any of those contractors have built or maintained other CMS public-facing systems that handle PII.
11. Please provide a complete explanation of:
    a. How SSNs came to reside in a public-facing database;
    b. What input validation or access controls were in place at launch;
    c. Why those controls failed to prevent or detect the exposure; and
    d. Who reviewed the system's data architecture before the information was published.
12. Has CMS completed a root cause analysis to identify the specific system vulnerability or process failure that resulted in this exposure? What mechanisms did CMS use to complete this analysis and which entities were involved? What has been determined to be the origin and mechanism of the breach, and what corrective actions have been implemented or are underway to prevent recurrence?

Remedies, Safeguards, and Independent Review

13. Has CMS offered affected providers with identity theft protection or other remedial services at no cost to the providers? If yes, identify the entity/entities providing the services. Has it been offered to all affected providers? How long will CMS provide the providers with these services?
14. Reporting suggests CMS is "reinforcing safeguards around data submission and validation." Please describe what CMS means by this and said safeguards.
15. In your March 2026 response, CMS stated that the temporary Medicare Advantage provider directory "does not replace the National Provider Directory initiative." Will CMS pause further expansion of the National Provider Directory pending (a) an independent security and accuracy review and (b) a referral to the U.S. Department of Health and Human Services Office of Inspector General? If not, explain why proceeding is appropriate given the documented failures identified above.

Any redactions made to the documents or information requested above should be accompanied by a privilege log identifying the document, the redacted material's category, and the basis for redaction. Blanket invocations will not be accepted.

Sincerely,

Jeffrey A. Merkley
United States Senator
Ranking Member, Committee on Budget

Ron Wyden
United States Senator
Ranking Member, Committee on Finance