

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

7500 Security Boulevard, Mailstop AR-18-50

Baltimore, Maryland 21244-1850



Date: September 3, 2024

To: All Medicare Advantage Organizations (MAOs) and Prescription Drug Plan Sponsors (PDPs)

From: Kathy Wolf, Group Director
Data Analytics and Systems Group, Center for Program Integrity

Re: Health Plan Portals: Potential Breaches and Unauthorized Access

The Centers for Medicare & Medicaid Services (CMS) has identified through social media monitoring and intelligence reports online communications discussing the sale of credentials and/or access to health plan provider portals by unauthorized individuals. Most of the communications are from individuals overseas (i.e. Pakistan, Egypt, and India) claiming to have access to, whether as health plan employees or as their capacity as health plan contractors to the health plan portals storing Protected Health Information (PHI). This is a similar pattern also identified within Traditional Medicare (Fee for Service) MAC provider portals, Medicaid portals and 3rd party Medicare Beneficiary Identifier (MBI) lookup tools.

Key Characteristics:

These individuals are primarily soliciting on LinkedIn and have the following attributes:

- **Call Center Groups with LinkedIn:** Individuals are part of Call Center groups within LinkedIn such as “USA Call Center Campaigns” and “USA Call Center Campaigns”.
- **Individuals Communicate with Specific “Hashtags” on LinkedIn:** The hashtags most communicated are #medb, #ppo, #hmo and #mbilookup. In addition, health plans are called out by name and the alleged level of access, whether selling or credentials or directly selling PHI from the health plan portal.
- **Individuals associated with Billing and Credentialing Agencies located in the United States (USA):** Certain individuals appear to have connections to billing and credentialing agencies in the USA remotely. Many of these billing and credentialing agencies are contractors for health plan credentialed providers.

Recommendations:

Increase oversight and proactive monitoring of provider portals at all major health plans across the program. Health plans should consider implementing proactive auditing and revising Terms of Use (TOU) and updating IT compliance plans to assist with identifying and mitigating the potential threat of data breach of PHI and unauthorized access to the provider portals.

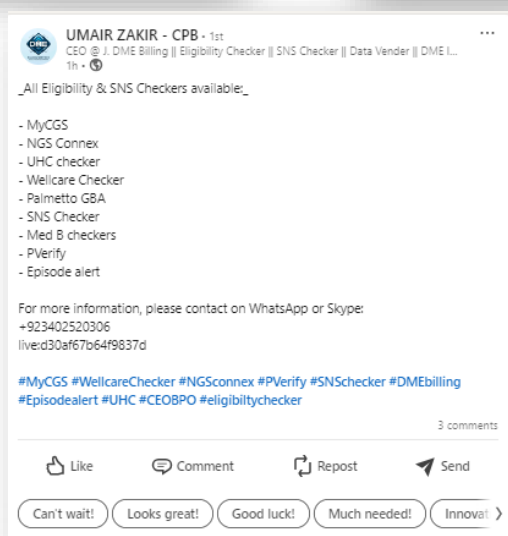
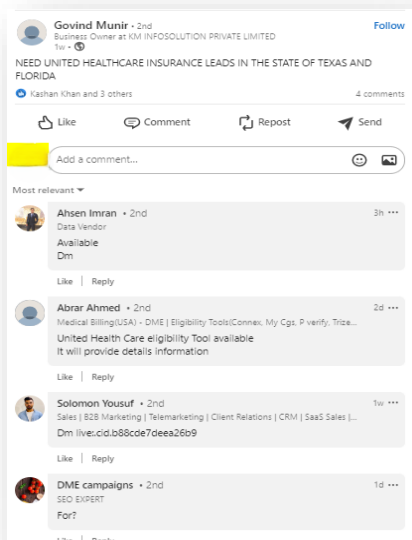
INFORMATION NOT RELEASABLE TO THE PUBLIC UNLESS AUTHORIZED BY LAW:

This information has not been publicly disclosed and may be privileged and confidential. It is for internal government use only and must not be disseminated, distributed, or copied to persons not authorized to receive the information. Unauthorized disclosure may result in prosecution to the full extent of the law.

For example, a proactive approach health plans could consider is monitoring of Internet Protocol addresses (IP addresses) to:

- Flag outlier amount of provider portal look ups by individuals overseas
- Consider use of suspension or revocation of usernames associated with suspicious access or lookups.
- Compare usernames, IP addresses and names on LinkedIn
- Identify and flag multiple IP addresses associated with one user credential. This could be indicative of selling access to established provider portal usernames and credentials for use by multiple unauthorized individuals.

Sample LinkedIn Screenshots:



INFORMATION NOT RELEASABLE TO THE PUBLIC UNLESS AUTHORIZED BY LAW:

This information has not been publicly disclosed and may be privileged and confidential. It is for internal government use only and must not be disseminated, distributed, or copied to persons not authorized to receive the information. Unauthorized disclosure may result in prosecution to the full extent of the law.