

CLARIFICATORY STATEMENT ON THE “URGENT NOTICE TO THE PUBLIC” ISSUED ON OCTOBER 03, 2023

In relation to the “Urgent Notice to the Public” that we published on October 3, 2023, we wish to reiterate and clarify the following:

1. The ransomware attack DID NOT affect our servers containing members’ private information. PhilHealth’s membership database, claims, contribution and accreditation information which are stored in a separate database are intact and completely unaffected by the said cyberattack.
2. Only the application servers and employees’ workstations have been affected by the said cyberattack. Hence, files stored locally in the hard drive of the infected workstations may have been compromised. An inventory is being conducted in order to determine the extent of information which may have been exfiltrated from these workstations.
3. The said Notice is in faithful and substantial compliance to the requirement of the National Privacy Commission to proactively reach out to and inform data subjects who may be affected by the malicious posts of the attackers. Likewise, this is a reminder to the public to stay vigilant in protecting personal and sensitive information.

We are actively reaching out to the public and the employees whose information may have been compromised. We are coordinating with Department of Information and Communications Technology (DICT), the National Privacy Commission (NPC), Philippine National Police (PNP) Cybercrime Division, Cybercrime Investigation and Coordinating Center (CICC) and the National Bureau of Investigation (NBI) in order to identify and go after the perpetrators of this criminal act.

We continue to appeal to our members to remain vigilant and to refrain from opening, sharing, liking, or reposting malicious posts as it only magnifies the damage caused by the perpetrators.

We value the trust reposed by our members in our Agency as we strengthen our information security measures to protect your right to data privacy. ###