National Privacy Commission

PhilHealthLeak Guidance No. 1

Heightened Vigilance Against Counterfeit PhilHealth IDs

The National Privacy Commission (NPC) issues this important Guidance to all Personal Information Controllers (PICs) and Personal Information Processors (PIPs). This Guidance underscores the urgent concern posed by the potential proliferation of counterfeit PhilHealth Identification Cards (IDs) in light of the recent #PhilHealthLeak incident.

On October 6, 2023, the Complaints and Investigation Division of the NPC concluded its initial analysis of the 650GB compressed data files linked to the Medusa Ransomware Group's data dump. It was determined that a portion of this data dump contained personal and sensitive personal information of PhilHealth members.

In light of these findings, the NPC strongly urges PICs and PIPs, particularly banks and non-bank financial institutions, hospitals, and public telecommunications entities (PTEs) to exercise heightened vigilance in detecting and preventing the fraudulent use of counterfeit PhilHealth IDs during various transactions.

In this regard, the NPC wishes to highlight the following risks unique and distinct to specific categories of PICs:

PICs/PIPs	Associated Risks
Banks and Non-Bank Financial Institutions	• **Identity Theft and Financial Fraud:** Fraudsters may exploit fake PhilHealth IDs to open fraudulent bank or financial accounts or conduct unauthorized financial transactions. This can lead to significant financial losses for both the bank and its customers. • **Money Laundering:** Counterfeit IDs can facilitate money laundering activities within the banking system, potentially exposing banks to legal and regulatory consequences.
Public and private hospitals	• **Medical Fraud:** Fraudulent IDs can be used to claim healthcare benefits and services, leading to unwarranted financial burdens on hospitals and potentially compromising patient care. • **Patient Data Breach:** The use of counterfeit IDs can result in unauthorized access to patient records and sensitive medical information, jeopardizing patient privacy and confidentiality.

Public telecommunication entities	• **Identity Theft in SIM Registration:** Counterfeit IDs may be used in the registration of SIM cards, enabling malicious actors to engage in criminal activities such as fraud, harassment, and scams while remaining anonymous.

The NPC reminds all concerned PICs, PIPs, and data subjects to take this advisory seriously and remain vigilant, refraining from any actions that could jeopardize their personal data. If anyone possesses information related to the use of counterfeit PhilHealth IDs, we kindly request you to contact us promptly at philhealthleak@privacy.gov.ph.

Your data privacy matters, and the NPC is here to protect it.

###