Republic of the Philippines
PHILIPPINE HEALTH INSURANCE CORPORATION
Citystate Centre, 709 Shaw Boulevard, Pasig City
Call Center (02) 441-7442 Trunkline (02) 441-7444
www.philhealth.gov.ph

PHILHEALTH CIRCULAR
No. 029 - 2015

TO : **ALL PHILHEALTH MEMBERS**

SUBJECT : **PHILHEALTH'S COMMITMENT TO ENSURE THE SECURITY OF MEMBERS' AND THEIR DEPENDENTS' PERSONAL INFORMATION**

I. RATIONALE

The Philippine Health Insurance Corporation (PhilHealth), in carrying out its mandate of administering the National Health Insurance Program (NHIP) pursuant to Republic Act. No. 7875 as amended by RA 9241 and 10606 otherwise known as the "The National Health Insurance Act of 2013" has gathered a considerable quantity of personal information. PhilHealth, being the custodian of such a huge quantity of personal information, has recognized the need to guarantee the commitment to the confidentiality and privacy of these personal information entrusted to us. As espoused in Section 16.q of RA 10606, it is the duty of the Corporation "to establish and maintain an electronic database of all its members and ensure its security to facilitate efficient and effective services." In consonance with the Data Privacy Act of 2012, the Corporation is committed to keeping its members' personal information confidential, secure, and private, and affirms the fundamental right of all persons, natural or juridical, with particular emphasis on its members and their dependents, to privacy.

II. OBJECTIVE

This issuance is intended to convey the Corporation's commitment towards confidentiality, integrity, and availability of personal information of all its members and their dependents. The Corporation follows security practices in compliance with laws and regulations, to continuously delight our members that will redound towards achieving our vision that "Bawat Pilipino, Miyembro; Bawat Miyembro, Protektado; Kalusugan Natin, Segurado!"

III. DEFINITION OF TERMS

The following terms are defined within the context of this issuance:

(1) **Personal Information** is defined "as any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual" (Data Privacy Act of 2012).

(2) **Privacy**, in constitutional law, is a constitutional right that protects the liberty of citizens to make certain decisions regarding their well-being without interference, coercion, intimidation from the government or other parties other than one's self.

(3) **Confidential Information** includes, but is not limited to, protected health information, personal financial information, patient records, or information gained from committee meetings, hospital or facility visits during accreditation and investigation, inquiries from members, patients or other PhilHealth employees. The definition is further expanded to include the following:

- ✓ Member and their dependents' personal and financial information including photographs and biometric identifiers, such as retinas or iris scans, fingerprints, voiceprints, or scan of hand for face geometry;
- ✓ Privileged health information, such as patient records, medical diagnoses, medical procedures, etc.; and
- ✓ Personal information of accredited health care professionals and providers, except those relating to the delivery of services or practice of profession, such as provider or clinic addresses, accreditation status, or duration of accreditation.

Confidential information may be in any form, format or medium, technology, and therefore, be disclosed in any such form, format or medium, and technology, including, but not limited to:

- ✓ Verbal or other human-to-human forms of communication;
- ✓ Handwritten notes or communications or machine printed hardcopies;
- ✓ Audio and/or video recordings;
- ✓ Electronic/machine-readable formats;
- ✓ Wired or wirelessly transmissible formats; and
- ✓ Any other unspecified form, format, media or technology for storing or sharing information.

The following terms are also defined in accordance with the definitions set by the National Institute of Standards and Technology (NIST)[1]:

(4) **Information security** means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(a) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;

(b) integrity, the protection of information from unauthorized access or revision, to ensure that the information is not compromised through corruption or falsification; and

(c) availability, which means ensuring timely and reliable access to and use of information.

[1] Federal Information Processing Standards Publication. (2004). Standards for Security Categorization of Federal Information and Information Systems. 2). Retrieved from http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

(5) **PhilHealth personnel** involves the entirety of PhilHealth's workforce i.e. all individuals working for, working in, and working at PhilHealth, or otherwise performing tasks in behalf of PhilHealth or for PhilHealth's benefit, regardless of rank, designation, status, tenure, terms of engagement or the existence or non-existence of an employee-employer relationship, with particular emphasis on those who have access to confidential information.

IV. COMMITMENT TO THE SECURITY OF MEMBERS' AND THEIR DEPENDENTS' INFORMATION

PhilHealth firmly commits to ensure and safeguard all member and their dependents' personal information consistent with the continuing advancement in technology.

A. Accountability

A.1. PhilHealth Personnel

All PhilHealth personnel must sign a Non-Disclosure Agreement (NDA) and are mandated to exert all reasonable efforts to restrict access to the barest minimum and to ensure that there is no unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction of confidential information. The NDA aims to ensure that all confidential information under PhilHealth's responsibility are treated with utmost level of confidentiality and security. Employees are likewise discouraged to divulge, copy, release, sell, alter or destroy confidential information except when properly authorized.

All PhilHealth personnel must abide by the Corporation's various information security policies in the handling of personal information. Each personnel is accountable for all personal information from his or her respective station and violations of instituted security policies are subject to disciplinary actions pursuant to applicable laws.

A.2. External Stakeholders

External stakeholders being engaged by the Corporation are likewise required to sign the NDA. External stakeholders include, but are not limited to, the following:

- ✓ Health Care Institutions and Health Care Professionals;
- ✓ Consultants, regardless of scope of work;
- ✓ IT specialists such as programmers, system analysts, and other specialists regardless of field of expertise;
- ✓ Individuals;
- ✓ Academic institutions;
- ✓ Government agencies and instrumentalities;
- ✓ Non-government organizations;
- ✓ International bodies and development organizations;
- ✓ Private entities or corporations and other similar individuals or entities, and;
- ✓ Vendors, suppliers, service of solution providers, private-public partners or prospective proponents.

Violations of instituted security policies for external stakeholders are subject to corresponding disciplinary actions pursuant to applicable laws.

B. Purpose of Collecting Personal Information

Personal information are collected for the following purposes:

A. To verify our member and their dependents' identity and protection against potential information security breaches. Security questions may be asked in the verification process;
B. To administer and update account records and respond to queries;
C. To provide appropriate services accorded to members and dependents; and
D. To comply with legal or regulatory requirements.

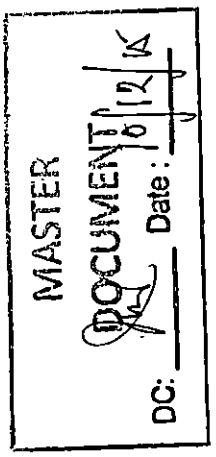
No person is allowed to collect personal information on behalf of the Corporation unless the collection is expressly authorized by an issuance, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

C. Member's Consent

The Corporation will ensure that the member and their dependents understand how their personal information will be used. A member's consent can be express or given through an authorized representative. Express consent may be provided in writing, orally, electronically or other appropriate means. The Corporation will not obtain consent through fraudulent practices.

D. Integrity of Member and Member Dependents' Information

To ensure and preserve the integrity of members' and their dependents' information that are being collected for the intended purposes, members should notify and inform the Corporation through any acceptable means if there are inaccuracies in their personal information e.g. misspelled names, incorrect date of birth, etc., or if there are changes in their personal information e.g. change in civil status, changes in membership category, *etc.* at the earliest possible opportunity so that the necessary changes are made promptly and accurately. Members are expected to perform the foregoing act to guarantee the veracity or integrity of the information saved in PhilHealth's database in aid of efficient availment and processing of PhilHealth benefits.



E. Measures to Secure Personal Information

The Corporation maintains appropriate measures to protect the sensitivity of the members' and dependents' personal information. The member's personal information is secure within the Corporation, regardless of the format in which it is held. The Corporation has evolving security policies and controls in place for protection against breaches in the confidentiality, integrity, and availability of personal information.

F. Awareness of Members on this Policy

The Corporation is transparent about the policies and procedures it uses to manage personal information. Members have access to information about these policies and procedures. This policy is available upon the member's request and is always available at the Corporate website (www.philhealth.gov.ph). The information will be made available in a manner that is generally easy to understand. From time to time, changes may ensue to this policy and inform members of changes.

G. Availability of Personal Information to Members

When members request in writing, along with providing satisfactory identification and proof of entitlement, the Corporation will, within a reasonable time, inform them what personal information the Corporation has, what it is being used for, and to whom it has been disclosed. The Corporation may need specific information about the member to enable the Corporation to search for, and provide the member with, the personal information that the Corporation holds about them.

V. LIMITATIONS FOR USING, DISCLOSING AND RETAINING PERSONAL INFORMATION

The Corporation will only use or disclose personal information for the reason(s) it was collected, unless the member gives an express consent to use or disclose it for another reason, or it is permitted or required by law.

Under certain exceptional circumstances, the Corporation has a legal duty or right to use or disclose personal information without the member's knowledge or consent to protect matters which include the Corporation or the public interest or in compliance with any law, governmental, judicial or administrative order, subpoena, discovery request, regulatory request or any similar means, unless such disclosure is in line with maintaining the transparency or accountability of a particular transaction entered into by PhilHealth. This is without prejudice to PhilHealth's right to seek a protective order or any other appropriate remedy in order to preserve the confidential nature of the information subject to disclosure.

Personal information or privileged health information of a member or their dependent may only be disclosed with the express consent of the member or member dependent, which shall be given full disclosure for its intended purpose.

VI. MONITORING AND EVALUATION

Monitoring shall be done by the office of the Regional Vice President/Branch Manager of PhilHealth Regional Offices (PROs) and Office of the Manager of Departments in the Head Office. The Corporate Information Security Department (InfoSec) shall perform oversight in the implementation of this policy. Reports shall be submitted to the Office of the President and CEO for actions deemed appropriate and necessary.

VII. SEPARABILITY CLAUSE

If any provision of this policy is declared unlawful, all other provisions which are not affected shall remain in effect and binding upon all parties concerned.

VIII. REPEALING CLAUSE

All provisions of previous issuances, circulars, and directives that are inconsistent with any of the provisions of this Circular are hereby amended, modified, or repealed accordingly.

IX. EFFECTIVITY

This circular shall take effect immediately.

for:

ALEXANDER A. PADILLA
President and CEO

Date Signed: 10/9/15

MASTER DOCUMENT
DC: ____ Date: 10/12/15