Policy Title	BSMH Data Privacy Act 2012 (DPA) Administrative Policy - Philippines
Policy Number:	None
Department:	Privacy - GBS
Contributing Department	Privacy
Approved by:	Chief Compliance Officer
Effective Date:	09/01/2025
Version:	2.0
Status:	Approved
Manual	Data Privacy Act - GBS
Section	Data Privacy Act - GBS

I. Mission, Vision and Values

This organization aims to ensure its Mission, vision, and values are reflected in all systemwide policies, procedures, and guidelines.

1. This policy reflects our commitment to human dignity by safeguarding individuals' rights to privacy and protecting their personal data.
2. This policy aligns with our mission to extend the compassionate ministry of Jesus and to enhance the health and well-being of our communities, by ensuring that data subjects in the Philippines—and any data processed within the country—are protected in accordance with Philippine laws.

II. Policy

This policy outlines BSMH's approach to manage, direct, enforce and protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth within the Philippines in accordance with the Data Privacy Act of 2012 (DPA).

III. Purpose

This policy establishes the standards and requirements for BSMH leaders and associates to ensure compliance with the Data Privacy Act (DPA) as implemented by the National Privacy Commission (NPC) of the Philippines.

It also outlines the rights of data subjects, emphasizing that the processing of personal information must be conducted transparently, for legitimate purposes, and in a manner that is proportional to those purposes.

IV. Scope

A. This policy applies to all entities within the Bon Secours Mercy Health, Inc. ("BSMH"), all BSMH Board Members, associates, contractors, agents, students, and providers (collectively referred to as "Covered Entity").

B. It applies to the processing of all types of personal information and covers all natural and juridical persons involved in such processing, including personal information controllers (PICs)and processors (PIPs) who handle the personal data of Philippine data subjects from outside the Philippines.

C. The policy also applies to any person that accesses personal data using equipment located in the Philippines or that maintains an office, branch, or agency within the country.

D. Additionally, this policy applies to BSMH associates in the United States who process personal information of individuals residing in the Philippines.

V. Policy Details

A. Rights of the Data Subject

1. The DPA requires BSMH adhere to the following standards regarding data subjects right to:

a) **Right to Be informed:** Data subjects have the right to be informed, prior to the collection and processing of their personal data, about the specific purpose of the processing, the legal basis, the duration of data retention, and any third parties with whom the data may be shared.

b) **Right to Obtain consent:** BSMH must obtain valid consent through written, electronic, or recorded means. Implied consent is not acceptable under the DPA.

c) **Right to Access and Correction:** Data subjects may request and receive a copy of the personal data held about them by a Personal Information Controller (PIC) or Personal Information Processor (PIP), and request correction of any inaccurate or outdated information.

d) **Right to Withdraw Consent:** Data subjects have the right to withdraw their consent at any time by making a formal request directly to the data controller.

e) **Right to Erasure or Blocking:** Individuals may request the erasure or blocking of their personal data if it is incomplete, outdated, false, unlawfully obtained, used without proper authorization, no longer necessary for the stated purpose, or if processing violates their rights.

f) **Right to Data Portability:** Data subjects may request a copy of their personal data in a structured, commonly used electronic format, provided it is based on their consent or a contract, and if the data controller has the technical capability to provide it.

g) **Right to Object:** Data subjects have the right to object to the processing of their data on legitimate grounds, including processing for direct marketing, automated decision-making, or profiling.

h) **Right to Damages:** If harm results from BSMH's non-compliance with the DPA, data subjects have the right to seek compensation for any resulting damages.

i) **Right to File a Complaint:** Data subjects may report suspected violations to:

i. **DPO** at DPOGBS@BSMHealth.org
ii. **GBS Manila Privacy and Compliance Concern Form**
iii. **National Privacy Commission (NPC) of the Philippines**

2. Data Protection Officer (DPO)

a) BSMH processes personal data in the Philippines and is therefore required to register with the National Privacy Commission (NPC) and designate a **Data Protection Officer (DPO).** The DPO plays a critical role in ensuring responsible management of personal data and in safeguarding the rights of data subjects.

b) The designated DPO for BSMH is accountable for ensuring the organization's compliance with the Data Privacy Act (DPA).

c) The DPO is responsible for monitoring BSMH's adherence to the DPA and its Implementing Rules and Regulations (IRR).

i. Key responsibilities of the DPO include:

i. Providing expert guidance on data protection matters;
ii. Advising on Data Protection Impact Assessments (DPIAs);
iii. Managing and responding to data breaches;
iv. Serving as the primary contact both data subjects and the NPC;
v. Conducting training and awareness programs for staff on data privacy requirements.

3. The **Compliance Officer for Privacy (COP)** is responsible for guiding and training associates on data privacy laws and BSMH policies, and for ensuring that third-party service providers comply with applicable privacy regulations.
    a) Key responsibilities of the COP include:
        i. Monitoring the organization's ongoing compliance with the Data Privacy Act (DPA), its Implementing Rules and Regulations (IRR), and other relevant issuances from the National Privacy Commission (NPC).
        ii. Identifying and assessing privacy risks related to new projects, systems, or processes.
        iii. Conducting privacy investigations, documenting findings, and reporting validated incidents to the Data Protection Officer (DPO).
        iv. Developing, reviewing, and updating privacy-related policies, guidelines, and programs to ensure alignment with current data protection laws and industry best practices.
        v. Serving as the primary point of contact for Personal Information Controllers (PICs) and Personal Information Processors (PIPs).

B. Training and Education
1. BSMH will provide mandatory new hire and annual training on the DPA laws and practices and will provide topical training as necessary.
2. Training may be provided in the web-based learning management system, in-person or otherwise virtually.
3. BSMH will maintain documentation of training.

C. Data Security Measures
1. BSMH Information Security is responsible for implementing appropriate technical, physical, and organizational measures to ensure the protection of personal data against unauthorized access, loss, or destruction. These measures include, but are not limited to:
    a) Implementation of strict access controls to limit data access to authorized personnel only;
    b) Use of encryption technologies to protect data in transit and at rest;
    c) Secure storage solutions for both digital and physical records;
    d) Mandatory employee training, as well as signed agreements outlining acceptable use, confidentiality,

D. Processing and Protecting Personal Data
1. BSMH associates shall process personal data in accordance with the Data Privacy Act (DPA), the Health Insurance Portability and Accountability Act (HIPAA), and all applicable BSMH policies and procedures.
    a) **Data Collection** – Personal data shall be collected only for legitimate, specified purposes and used solely for the purpose for which it was collected.
    b) **Use of Data** – Personal data shall be used strictly to fulfill necessary business-related functions and only for purposes that have been properly authorized.
    c) **Data Storage, Retention, and Destruction** – Personal data must be securely stored, retained only for the minimum duration necessary, and permanently destroyed in a safe manner once no longer required.
    d) **Data Access** – Access to personal data shall be restricted to associates who require it to perform their job duties. No individual may access personal data without a valid, approved business purpose.
    e) **Disclosure and Sharing** – All associates are required to maintain the confidentiality of personal data encountered in the course of their duties. This obligation continues even

after resignation, termination, or the conclusion of any contractual relationship. Personal data may only be disclosed when required by law and shared with authorized recipients for lawful purposes.

E. Privacy Notices
   1. BSMH physical locations where personal data of Philippine data subjects are processed must display a Philippine **Privacy Notice**. This requirement applies to any location, whether within the Philippines or abroad, where the data subjects are Filipino individuals.
      a) The notice must be written in clear, accessible language and must include: the name of the data controller, the purpose of data processing, the types of personal data being collected, the scope and duration of processing, the rights of data subjects under the Data Privacy Act (DPA), and instructions on how to exercise those rights.
      b) The privacy notice should inform U.S. data subjects of the processing activities, the basis for processing, the purposes of processing, the recipients of the data (including the Philippine location), and the existence of their rights under both U.S. and Philippine laws.
   2. As a covered entity, any BSMH location in the Philippines that processes the personal information of U.S. data subjects must also display a **Notice of Privacy Practices** and ensure that all processors comply with HIPAA Privacy Rule requirements.

F. Reporting DPA or other potential violations
   1. BSMH associates, vendors, contractors, and agents are expected to report suspected or actual violations of the DPA immediately to Compliance.
      a) If you see or hear anything that seems inconsistent with the Code, applicable laws, regulations, or internal policies or if you have concerns about data creation, collection, storage, processing, usage, destruction, access or sharing, report concerns to the Data Privacy Officer (DPO) at DPOGBS@BSMHealth.org.
      b) Speak to the Compliance Officer for Privacy (COP).
      c) Contact Compliance directly via email at DPOGBS@BSMHealth.org.
      d) **Call the 24/7 toll-free BSMH Ethics Help Line at 1800-1-322-0316 or submit an On-line report at** GBS-Manila Privacy and Concern Form**.** You may remain anonymous.
   2. BSMH must provide NPC an initial notification within **72 hours** of discovering a breach involving sensitive personal information or a high risk of harm,
   3. Followed by a full report within **5 days** from the date of discovery, unless granted an extension.

G. Breach and Security Incidents
   1. BSMH shall implement procedures to prevent, detect and mitigate breach and security incidents.
      a) PICs or PIPs are required to establish and maintain comprehensive policies and procedures for managing personal data breaches and security incidents. These must include:
         i. Establishment of a Data Breach Response Team
            i. A dedicated team composed of five (5) designated officers responsible for ensuring immediate and coordinated action to contain and mitigate the impact of any breach or security incident.
         ii. Preventive and Risk-Reduction Measures
            a. Implementation of safeguards and practices designed to minimize the likelihood and impact of breaches or incidents.
         b. Data Recovery and Restoration Procedures

a. Defined processes for restoring personal data, including the use of backup files and systems, to ensure business continuity and data integrity.

c. Notification Protocol
   a. The Head of the Data Breach Response Team shall assess the breach and, if required by law, notify the National Privacy Commission (NPC) and affected data subjects within the timeframe prescribed under the Data Privacy Act.

d. Documentation and Reporting
   a. All breaches and security incidents must be thoroughly documented. The Data Breach Response Team shall prepare detailed incident reports and an annual summary report for submission to BSMH management and the NPC, in accordance with regulatory deadlines.

VI. Definitions

Data Subject– refers to an individual whose personal, sensitive personal or privileged information is processed by the organization. It may refer to officers, employees, consultants, and clients of this organization.

Personal Information/ Personal Data – refers to 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.

Processing - refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

Personal Information Processor (PIP) – refers to an entity that processes personal information on behalf of a data controller.

Personal Information Controller (PIC) - whether an individual, organization, or public authority—that determines the purposes and means of processing personal data. They decide why and how personal information is collected, held, used, and disclosed and bear the legal responsibility for ensuring that these activities comply with data protection laws and principles.

VII. Attachments

N/A

VIII. Related Policies

HIPAA Privacy
Notice of Privacy Practices Policy
Reporting Compliance Concerns / Non-Retaliation Policy
Safeguarding and Storing Protected Health Information (PHI) Policy
Compliance Investigations
Compliance Training and Awareness
Acceptable Use Policy
Confidentiality and Security

IX. Regulatory Notices

Nothing in this policy modifies the at-will status of any organizational associate or otherwise creates a contractual relationship between the organization and any associate.

The organization, in its sole discretion, reserves the right to amend, terminate or discontinue this policy at any time, with or without advance notice.

X. Version Control

Version	Effective Date	Next Review Date	Description	Supersedes, if applicable	Prepared By
1.0	09/01/2025	09/01/2027	New Policy - Philippines DPA laws effective for Manila		Data Protection Officer - Manila
2.0	09/16/2025	09/01/2027	Corrected template header and added Right to File a Complaint	1.0	Data Protection Officer - Manila

This policy/procedure/guideline is not intended to establish a standard of clinical or non-clinical care or practice. Rather, this policy/procedure/guideline creates a general tool to help guide decision-making with the understanding that different action(s) may be necessary in response to the totality of the circumstances presented.

Sites revised 05/06/2025- Bon Secours Mercy Health adopts the above policy, procedure, policy & procedure, guideline, manual / reference guide / instructions, or principle / standard / guidance document for all Bon Secours Mercy Health entities including, but not limited to, facilities doing business as Mercy Health – St. Vincent Medical Center, St. Vincent – St. Charles Hospital, St. Vincent – St. Anne Hospital, Mercy Health – Perrysburg Medical Center, Mercy Health – Tiffin Hospital, Mercy Health – Willard Hospital, Mercy Health – Defiance Hospital, Mercy Health Allen Hospital LLC, Mercy Health - Lorain Hospital, Mercy Health St. Elizabeth Youngstown Hospital, Mercy Health St. Joseph Warren Hospital, Mercy Health - St. Elizabeth Boardman Hospital, Mercy Health - St. Rita's Medical Center, Mercy Health – Springfield Regional Medical Center, Mercy Health - Urbana Hospital, Mercy Health - Anderson Hospital, Mercy Health - Clermont Hospital, Mercy Health – Fairfield Hospital, Mercy Health - West Hospital, The Jewish Hospital – Mercy Health, Mercy Health – Kings Mills Hospital, LLC, Mercy Health - Lourdes Hospital LLC, Mercy Health – Marcum and Wallace Hospital, Chesapeake Hospital Corporation DBA Rappahannock General, Maryview Hospital, Bon Secours Richmond Community, Bon Secours Memorial Regional Medical Center, Bon Secours – St. Mary's Hospital, Bon Secours St. Francis Health System, Bon Secours St. Francis Medical Center, Bon Secours Mary Immaculate Hospital, Bon Secours - Southside Medical Center, Bon Secours Mercy Health Franklin, LLC, Southern Virginia Medical Center, and Bon Secours Harbour View Medical Center. This also may apply to Bon Secours Mercy Health Medical Group LLC and its medical group affiliates.