SOCIETY OF GYNECOLOGIC ONCOLOGISTS OF THE PHILIPPINES FOUNDATION, INC. (SGOP)

Data Privacy Manual

ARTICLE I. Background

Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), aims to protect personal data in information and communications systems both in the government and the private sector.

It ensures that entities or organizations processing personal data establish policies and implement measures and procedures that guarantee the safety and security of personal data under their control or custody, thereby upholding an individual's data privacy rights. A personal information controller or personal information processor is instructed to implement reasonable and appropriate measures to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

To inform its personnel of such measures, each personal information controller or personal information processor is expected to produce a Data Privacy Manual. The Manual serves as a guide or handbook for ensuring the compliance of an organization or entity with the DPA, its Implementing Rules and Regulations (IRR), and other relevant issuances of the National Privacy Commission (NPC). It also encapsulates the privacy and data protection protocols that need to be observed and carried out within the organization for specific circumstances (e.g., from collection to destruction), directed toward the fulfillment and realization of the rights of data subjects.

ARTICLE II. Introduction

This Data Privacy Manual is hereby adopted in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations, and other relevant policies, including issuances of the National Privacy Commission. This organization respects and values your data privacy

rights and make sure that all personal data collected from you, our clients and customers, are processed in adherence to the general principles of transparency, legitimate purpose, and proportionality.

This Manual shall inform you of our data protection and security measures and may serve as your guide in exercising your rights under the DPA.

ARTICLE III. Definition of Terms

3.1 **Authorized personnel** – refers to employees or officers of the SGOP specifically authorized to collect and/or to process personal information either by the function of their office or position, or through specific authority given in accordance with the policies of the SGOP.

3.2 **Data Subject** – refers to an individual whose personal, sensitive personal or privileged information is processed by the SGOP. For purposes of this Manual, members, employees, applicants, patients, visitors and other third parties whose information is being collected and processed by the SGOP are the data subject.

3.3 **Consent of the data subject** – refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal or privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so.

3.4 **Data Protection Officer or DPO** – refers to the officer of the SGOP designated in order to monitor and ensure the compliance of the SGOP with the Data Privacy Act. The DPO is also the head of the Breach Management Response Team and the contact officer of the National Privacy Commission.

3.5 **Data Breach Management Response Team** – refers to the group of persons designated to respond to inquiries and complaints relating to data privacy and to assist in the monitoring and implementation of the

Data Privacy Policy of the SGOP. The Data Breach Management Response Team is composed of members who will be assigned by the Board of Trustees.

3.6 **Personal Information** – 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.

3.7 **Personal Information Controller or PIC** - refers to a natural or juridical person, or any other body who controls the processing of personal data or instructs another to process personal data on its behalf.

3.8 **Personal Information Processor or PIP** - refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject.

3.9 **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.

3.10 **Privacy Statement** - a notification or statement, in the format specified herein to an individual informing him/her of the use and purpose for collecting or processing the information, and/or which allows such individual to consent to such processing of information.

3.11 **Privileged information** - refers to information received on account of a special relationship protected by law.

3.12 **Security incident -** refers to an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data.

3.13 **Sensitive personal information** refers to personal information about an individual's:

3.13.1 Race, ethnic origin, marital status, age, color and religious, philosophical or political affiliations;

3.13.2 Health, education, genetic or sexual life or involvement to any proceeding for an offense committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

3.13.3 Identification numbers issued by government agencies peculiar to an individual which includes but are not limited to social security numbers, tax returns and identification numbers, health records, licenses or its suspension, revocation or denials.

3.14 **Member records -** refers to the records of members of all acts, events, accomplishments, results, research and all documents depicting the various activities of the members. These include but are not limited to the following:

3.14.1 Personal and academic records of members
3.14.2 Professional development reports
3.14.3 Disciplinary records
3.14.4 Financial records within the SGOP

3.15 **SGOP personnel** - refer to all employees regardless of the type of employment or contractual arrangement of the SGOP.

ARTICLE IV. Scope and Limitations

All personnel of the SGOP, regardless of the type of employment or contractual arrangement, members, officers, and third parties must comply with the terms set out in this Data Privacy Manual. The data covered by this Manual is limited to personal information and sensitive personal information as defined under Article III, which are being processed by the SGOP.

ARTICLE V. Collection of Personal Data

The SGOP collects the basic contact information of its members, employees, applicants and third parties, including their full name, address, email address,

contact numbers, together with other sensitive personal information deemed necessary for purposes set out in this Manual.

5.1 DATA PRIVACY PRINCIPLES ESPOUSED BY THE SGOP

A. TRANSPARENCY. The consent of the data subject shall be obtained prior to the collection of his/her personal data and the latter should be informed of the nature, purpose and extent of the processing of his/her personal data.

B. LEGITIMACY. The processing of the personal data shall be compatible with the declared and specified purpose and shall not be contrary to law, morals or public policy.

C. PROPORTIONALITY. The personal data collected is adequate, relevant, suitable, necessary and not excessive in relation to the declared and specified purpose.

5.2 PROVISIONS FOR SPECIFIC COMMITTEES

A. Committee on Tumor Registry

The Tumor Registry collects personal and sensitive personal information of patients with gynecologic cancer as well as social and/or personal history and treatment they received. This information is used to generate data on prevalence/ incidence, stage, survival outcomes of the different gynecologic malignancies per organ site (e.g. cervix, uterus, ovary, fallopian tube, vulva, vagina).

In the course of the collection of information, the authorized personnel from the said committee ask data subjects to fill out forms with the corresponding privacy statement to signify consent and to inform them of the purpose of collecting such information during the admission and evaluation processes. The committee collect and process the information and encode the same in the website registry which is being processed by a Personal

Information Processor (PIP) outsourced by the SGOP. Only authorized personnel are allowed to encode and access patients' data.

Access is restricted pursuant to the provisions of the SGOP's policies and the Outsourcing Agreement with the PIP which specifically provides that patient records should be kept strictly confidential.

B. Committee on Credentials and Membership

The Committee on Membership collects personal information for the purpose of periodic review of the current status of members, recommend ways and means to ensure active membership to the SGOP, recommend to the Board of Trustees candidates for eligibility to become a diplomate or fellow and deliberate on financial delinquency cases submitted to it by the Finance Committee and recommend proper disciplinary action.

In the course of the collection of information, the authorized personnel from the said committee ask data subjects to fill out forms with the corresponding privacy statement to signify consent and to inform them of the purpose of collecting such information during the admission and evaluation processes. The committee collect and process the information and encode the same in the SGOP's computer files and manual filing section. Only authorized personnel are allowed to encode and access applicants and members data.

Access is restricted pursuant to the provisions of the SGOP By-laws, policies and procedures which specifically provides that all applicants and member records should be kept strictly confidential.

C. Committee on Finance

The Committee on Finance collects personal information for the purpose of ascertaining the financial obligations of members with respect to their status in the SGOP.

In the course of the collection of information, the authorized personnel from the said committee ask data subjects to fill out forms with the corresponding privacy statement to signify consent and to inform them of the purpose of collecting such information during the preparation and coordination processes. The committee collect and process the information and encode the same in the manual filing system. Only authorized personnel are allowed to encode and access applicants and members data.

Access is restricted pursuant to the provisions of the SGOP By-laws, policies and procedures which specifically provides that all applicants and member records should be kept strictly confidential.

D. Committee on Research

The Committee on Research collects personal information for the studies and research of the members of SGOP consistent with the National Health Program and assistance to members and residents and fellows in training for outstanding scientific work.

In the course of the collection of information, the authorized personnel from the said committee ask data subjects to fill out forms with the corresponding privacy statement to signify consent and to inform them of the purpose of collecting such information during the admission and evaluation processes. The committee collect and process the information and encode the same in the manual filing system. Only authorized personnel are allowed to encode and access applicants and members data.

Access is restricted pursuant to the provisions of the SGOP By-laws, policies and procedures which specifically provides that all records should be kept strictly confidential.

E. Informatics Committee

The Informatics Committee collects personal information for the maintenance of the SGOP website and the various activities of the SGOP done virtually or through online communication.

In the course of the collection of information, the authorized personnel from the said committee ask data subjects to fill out forms with the corresponding privacy statement to signify consent and to inform them of the purpose of collecting such information during the admission and evaluation processes. The committee collect and process the information and encode the same in the SGOP cloud-based servers. Only authorized personnel are allowed to encode and access applicants and members data.

Access is restricted pursuant to the provisions of the SGOP By-laws, policies and procedures which specifically provides that all personal and sensitive personal information should be kept strictly confidential and accessed only by authorized personnel.

F. Committee on Library and Archives

The Committee on Library and Archives collects personal information including but not limited to pictures, audio recordings and videos for the documentation of all SGOP activities over the course of its existence.

In the course of the collection of information, the authorized personnel from the said committee ask data subjects to fill out forms with the corresponding privacy statement to signify consent and to inform them of the purpose of collecting such information during the admission and evaluation processes. The committee collect and process the information and encode the same in the SGOP cloud-based servers. Only authorized personnel are allowed to encode and access applicants and members data.

Access is restricted pursuant to the provisions of the SGOP By-laws, policies and procedures which specifically provides that all personal and sensitive personal information should be kept strictly confidential and accessed only by authorized personnel.

G. Secretariat

The Secretariat collects the information from employees or applicants for purposes of evaluating the applicant for eligibility for employment, and availing of employee benefits (i.e. retirement and medical benefits) and collates the information in the individual 201 files of the employees which is required under the provisions the Labor Code.

Pursuant to existing labor laws and human resources policies of the Society, the 201 files or employee's individual employment records are confidential and access is restricted to authorized personnel only.

Personal information collated needed in the transaction of business of the members with the society (e.g. courier services for transport of documents etc.) are restricted to authorized personnel of the Society.

H. Philippine Board of Gynecologic Oncology

The Board collects personal information of examinees and patients that are anonymized for the purpose of evaluating their eligibility to become a fellow or diplomate. Upon completion of certifying exams, all these documents are discarded.

In the course of the collection of information, the authorized personnel from the said board ask data subjects to fill out forms with the corresponding privacy statement to signify consent and to inform them of the purpose of collecting such information during the admission and evaluation processes. The board collect and process the information and encode the same in the Microsoft Access and manual filing system. Only authorized personnel are allowed to encode and access applicants and members data.

Access is restricted pursuant to the provisions of the guidelines of the Philippine Board of Gynecologic Oncology which specifically provides that all applicants and member records should be kept strictly confidential.

ARTICLE VII. Use of Information

Authorized SGOP personnel are allowed to access, use and process said information for legitimate primary or secondary purposes of the SGOP and/or that which is stated in the privacy statement contained in the forms or documents signed by the members or employees.

6.1 PRIMARY PURPOSE

The SGOP is a non-stock, non-profit professional organization of gynecologic oncologist and specialists of related disciplines committed to the continuous upgrading of the standards of practice, teaching, research in the field of gynecologic oncology in the Philippines resulting in a Filipino nation free of gynecologic cancer. All personal data is to be processed and used by authorized personnel for such purposes.

6.2 SECONDARY PURPOSES

Secondary purposes are those which are collateral to the primary purposes and which are necessary to process the information. These include monitoring the current administrative or disciplinary standing for member and employee discipline, financial condition or the health and psychological wellness of members and employees. Authorized SGOP personnel are allowed to use personal information collected and/or processed for such purposes provided the following circumstances are present:

6.2.1 The member or employee has consented in writing to the use or disclosure for the secondary purpose; or

6.2.2 The member or employee would reasonably expect the SGOP through its authorized personnel to use, or process personal information for secondary purpose and that the secondary purposes are directly related to the primary purposes.

6.3 SENSITIVE PERSONAL INFORMATION

Sensitive personal information may not be disclosed or processed, except in any of the following cases:

6.3.1 Written consent is given by data subject, prior to the processing of the sensitive personal or privileged information, which shall be undertaken pursuant to a declared, specified, and legitimate purpose of the SGOP.

6.3.2 The processing of the sensitive personal information provided for by existing laws and regulations provided, that said laws and regulations do not require the consent of the data subject for the processing and guarantee the protection of personal data.

6.3.3 The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing.

6.3.4 The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations provided that the processing is confined and related to the bona fide members of these organizations or their associations; the sensitive personal information are not transferred to third parties; and consent of the data subject was obtained prior to processing.

6.3.5 The processing is necessary for the purpose of medical treatment, carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal data is ensured.

6.3.6 The processing concerns sensitive personal information or privileged information necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority pursuant to a constitutional or statutory mandate.

ARTICLE VIII. Storage, Retention and Destruction of Information

The SGOP will ensure that personal data under its custody are protected against any accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing. The SGOP will implement appropriate security measures in storing collected personal information, depending on the nature of the information. All information gathered shall not be retained for more than fifty (50) years from the date of collection of the personal data.

ARTICLE IX. Access to Information

Due to the sensitive and confidential nature of the personal data under the custody of the SGOP, only the members and the authorized representative of the SGOP shall be allowed to access such personal data, for any purpose, except for those contrary to law, public policy, public order or morals.

ARTICLE X. Disclosure and Sharing of Information

All employees and personnel of the SGOP shall maintain the confidentiality and secrecy of all personal data that come to their knowledge and possession, even after resignation, termination of contract, or other contractual relations. Personal data under the custody of the company shall be disclosed only pursuant to a lawful purpose, and to authorized recipients of such data.

Personal information is allowed to be used and disclosed to government agencies to satisfy reportorial requirements in line with their constitutionally or legislatively mandated functions pursuant to existing medical or labor laws or when the use is pursuant to lawful order of the court or tribunal.

ARTICLE XI. Security Measures

As a personal information controller, the SGOP implements reasonable and appropriate physical, technical and organizational measures for the protection of personal data. Security measures aim to maintain the availability, integrity

and confidentiality of personal data and protect them against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

1. ORGANIZATION SECURITY MEASURES

1.1 Data Protection Officer (DPO)

The designated Data Protection Officer is Dr. Lilli May Teodoro-Cole, who is concurrently serving as the Vice President of the SGOP.

1.2 Functions of the DPO, COP and/or any other responsible personnel with similar functions

The Data Protection Officer shall oversee the compliance of the organization with the DPA, its IRR, and other related policies, including the conduct of a Privacy Impact Assessment, implementation of security measures, security incident and data breach protocol, and the inquiry and complaints procedure.

1.3 Conduct of trainings or seminars to keep personnel, especially the Data Protection Officer updated vis-à-vis developments in data privacy and security

The SGOP shall sponsor a mandatory training on data privacy and security at least once a year. For personnel directly involved in the processing of personal data, management shall ensure their attendance and participation in relevant trainings and orientations, as often as necessary.

1.4 Conduct of Privacy Impact Assessment (PIA)

The SGOP shall conduct a Privacy Impact Assessment (PIA) relative to all activities, projects and systems involving the processing of personal data. It may also choose to outsource the conduct a PIA to a third party.

1.5 Recording and documentation of activities carried out by the DPO, or the organization itself, to ensure compliance with the DPA, its IRR and other relevant policies.

The SGOP shall sponsor a mandatory training on data privacy and security at least once a year. For personnel directly involved in the processing of personal data, management shall ensure their attendance and participation in relevant trainings and orientations, as often as necessary. The said personnel shall be required to submit a written report on their attendance to the said trainings and ensure that the same is kept in file for future reference of other authorized personnel.

1.6 Duty of Confidentiality

All employees (including the Board of Trustees, officers) will be asked to sign a Non-Disclosure Agreement. All employees with access to personal data shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.

1.7 Review of Privacy Manual

This Manual shall be reviewed and evaluated annually or depending on when the need arises. Privacy and security policies and practices within the SGOP shall be updated to remain consistent with current data privacy best practices.

2 PHYSICAL SECURITY MEASURES

Personal data under the control and custody of SGOP is collected, processed and stored in either paper or hard copy format or electronically stored in local storage or shared storage (server or cloud-based).

PHYSICAL SECURITY MEASURES	HARD COPY STORAGE	LOCAL STORAGE	SHARED STORAGE
Storage Type	Secured filing cabinets	Local hard drives, External hard drives, USB	Google Shared Drive Cloud based

Location	Locked cabinets located in the SGOP office	PCs located in the offices of authorized personnel	Google Shared Drive Cloud based
Access procedures	Keys and access to locked offices available only to authorized personnel	Keys and access to locked offices available only to authorized personnel	Only authorized SGOP personnel have access to Google shared drive. (2-step verification)
Monitoring & limitation	Offices are locked when unattended	Offices are locked when unattended	Archives Committee and Secretary of the SGOP.
Workspace design		The computers are positioned with considerable spaces between them to maintain privacy and protect the processing of personal data.	
Data transfer	Only done with proper authorization		Only done with proper authorization
Retention and Disposal	For as long as necessary	For as long as necessary	For as long as necessary

3 TECHNICAL SECURITY MEASURES

The SGOP, as a personal information controller and personal information processor, shall implement technical security measures to make sure that there are appropriate and sufficient safeguards to secure the processing of personal data, particularly the computer network in place, including encryption and authentication processes that control and limit access. They include the following, among others:

User access rights

1. All SGOP members known as "*Users*" are given specific access rights based on their respective roles/committees.

2. The User has the right to access, review and request a physical or electronic copy of information. The User also has the right to request information on the source of Personal Data.

3. These rights can be exercised by sending a formal request through e-mail to the Data Privacy Officer and stating therein the purpose(s) for such request. If the request is submitted by a person other than the SGOP member, without providing the proper authorization letter that the request is legitimately made on behalf of the User, the request will be rejected.

4. For authorized representatives, he/she must be with equipped with a Special Power of Attorney in order to access or process any personal information of the SGOP members he/she representing.

Control and limit access to personal data

Username and password will be provided to the Data Privacy Officer and the Data Processor in-charge of the project. Only the Data Privacy Officer has the access and power to provide additional access rights to anyone within the SGOP Office.

Access to the data server may be granted only upon the consent of the Data Privacy Officer, or upon approval of the Board.

Data Transfer

No personal information may be transferred, in any form, without the consent of the Data Privacy Officer and the Board.

In all cases, the transfer of any information of a data subject through hard copy shall be delivered to the designated person through sealed

envelopes marked with “confidential”, without prejudice to any agreement approved by the Board.

Transfer of electronic information shall be done only upon approval of the DPO and the Board through devices issued by the SGOP.

Monitoring for security breaches

1. Official SGOP website has specific software that records and denies unauthorized access by blocking IP address after three (3) wrong passwords to prevent hacking.

2. The DPO and Data Breach Response Team shall be responsible in managing security incidents and/or data breaches involving information of SGOP members.

3. Control over the data server where the information of the data subjects shall be subject to the control and discretion of the SGOP through the Board and/or DPO.

4. The Developer, and all its employees, who are involved in the maintenance of the servers are tasked with regularly monitoring for signs of a possible data breach or security incident. In the event that such signs are discovered, the employee shall immediately report the facts and circumstances to the DPO not later than twenty-four (24) hours from his or her discovery for verification as to whether or not a breach requiring notification under the Data Privacy Act has occurred as well as for the determination of the relevant circumstances surrounding the reported breach and/or security incident. The DPO shall notify the National Privacy Commission and the affected data subjects pursuant to requirements and procedures prescribed by the DPA.

5. The notification to the DPA and the affected data subjects shall include the following information:

    a. nature of the breach;
    b. the personal data possibly involved;

c. the measures taken by the Office to address the breach;
d. the measures taken to reduce the harm or negative consequences of the breach; and
e. the name and contact details of the DPO.

6. The form and procedure for notification shall conform to the regulations and circulars issued by the National Privacy Commission, as may be updated from time to time.

Security features of applications(s)

Websites developed are installed with SSL (Secured Socket Layer) for data encryption to ensure that Personal Data submitted by users are secured.

Regular testing and assessment of security measures

The Developer quarterly conducts website security scanning to determine if website security is compromised. They shall also quarterly apply software patches on the web server software to make sure versions are up-to-date.

ARTICLE XII. Breach and Security Incidents

1. Creation of a Data Breach Response Team

The Data Breach Response Team shall be composed of:

a) Chair, Committee on Library and Archives
b) Chair, Committee on Informatics
c) Chair, Committee on Tumor Registry
d) Vice-President and Chair, Credentials and Membership
e) President

The team shall be responsible for ensuring immediate action in the event of a security incident or personal data breach. The team shall conduct an initial assessment of the incident or breach in order to ascertain the nature

and extent thereof. It shall also execute measures to mitigate the adverse effects of the incident or breach.

2. **Measures to prevent and minimize occurrence of breach and security incidents**

   The SGOP shall regularly conduct a Privacy Impact Assessment to identify risks in the processing system and monitor for security breaches and vulnerability scanning of computer networks. Personnel directly involved in the processing of personal data must attend trainings and seminars for capacity building. There must also be a periodic review of policies and procedures being implemented in the organization.

3. **Procedure for recovery and restoration of personal data**

   The SGOP shall always maintain a backup file for all personal data under its custody. In the event of a security incident or data breach, it shall always compare the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the incident or breach.

4. **Notification protocol**

   The Head of the Data Breach Response Team shall inform the management of the need to notify the NPC and the data subjects affected by the incident or breach within the period prescribed by law. Management may decide to delegate the actual notification to the head of the Data Breach Response Team.

5. **Documentation and reporting procedure of security incidents or a personal data breach**

   The Data Breach Response Team shall prepare a detailed documentation of every incident or breach encountered, as well as an annual report, to be submitted to management and the NPC, within the prescribed period.

ARTICLE XIII. Inquiries and Complaints

Every data subject has the right to reasonable access to his or her personal data being processed by the personal information controller or personal information processor. Other available rights include: (1) right to dispute the inaccuracy or error in the personal data; (2) right to request the suspension, withdrawal, blocking, removal or destruction of personal data; and (3) right to complain and be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data. Accordingly, there must be a procedure for inquiries and complaints that will specify the means through which concerns, documents, or forms submitted to the organization shall be received and acted upon. This section shall feature such procedure.

Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of the Society, including the data privacy and security policies implemented to ensure the protection of their personal data. They may write to the organization addressed to the Data Protection Officer and briefly discuss the inquiry, together with their contact details for reference.

Complaints shall be filed in three (3) printed copies sent to Rm 414 Manila Astral Tower 1330 Taft Ave cor Padre Faura St. Ermita Manila or through email at _____. The Data Protection Officer shall confirm with the complainant its receipt of the complaint.

ARTICLE XIV. Effectivity

The provisions of this Manual are effective this __ day of _____, 2022, until revoked or amended by this SGOP through a Board Resolution**.**