HIPAA and Privacy SOP

1. Purpose

This procedure describes VPG's approach to protecting personal information.

2. Scope

This SOP applies to all VPG personnel and all projects.

3. References

- Privacy Notice Form (QS-01-TPL-03)
- Health Insurance and Portability and Accountability Act (HIPAA) Checklist (QS-01-TPL-02)
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996)

4. Responsibilities

4.1. All VPG Employees

All VPG employees are responsible for following this procedure.

4.2. Chief Executive Officer or Chief Technology Officer

The Chief Executive Officer (CEO) or the Chief Technology Officer (CTO) or designee is responsible for notifying customers of breaches. They are also responsible for enforcing this procedure and documenting any breaches, notifying any regulatory authorities of any breaches, as well as administering and updating this procedure. As well as being responsible for notifying employees of the use of their personal information. The CEO and CTO or designee is responsible for receiving any breaches and for following them through to resolution.

5. Definitions

Term	Changes
Personal Information	Identifying information that is recorded in any form, is about or pertains to a specific individual, and can be linked to that individual. Examples include name, initials, home and personal e-mail address, phone number, DOB, DOD, and facial pictures or videos, fingerprints. Data that have been anonymized are not considered Personal Information.
Sensitive Personal Information	Financial, legal and other personal information, such as SSN, credit background, race, nationality, sexual orientation, political opinions, religious affiliation, philosophical beliefs, trade union membership, medical records and condition of health.
Business Contact Information	Information such as name, job title, company name, business address, business phone/fax/pager, and business email address.

6. Procedure

6.1. Employee Personal Information: Collection and Notification of Use

VPG collects Personal Information and Sensitive Personal Information from employees to meet legal and regulatory requirements and to process employee pay and benefits.

During employee orientation VPG notifies its employees via the Privacy Notice Form (QS-01-TPL-03) about the purposes for which it collects and uses information about them and the third parties to whom such information will be disclosed. Employees are required to sign and date the Privacy Notice Form and include it in their training file.

Employees shall check their personal information for accuracy and inform the CEO/Vice President in writing if they desire to explicitly opt out of disclosure of Personal Information to designated third parties for whom they do not wish to give authorization. All employees will be opted in for disclosure of Sensitive Personal Information to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual unless otherwise noted.

Employees can contact the CEO or CTO with any questions about the use of Personal Information.

6.2. Customer Related Personal Information: Receipt and Notification

Since it is normal business conduct to exchange business contact information (e.g., business cards), such contact information is not Personal Information and is not protected by this SOP.

An employee will not offer such business contact information to a third party without that person's permission.

VPG may be required to receive both Personal and Sensitive Personal Information of patients/subject/users to perform our services. If such information is transmitted to VPG and is found not to pertain to a contracted

project, the person receiving such information will notify CEO or CTO. The CEO or CTO or designee will in turn notify the sender and any applicable regulatory body of the occurrence (Section 6.5).

6.3. Customer Related Personal Information: Third Parties' Privacy Assurance

If it is necessary to involve a third party in the collection, analysis, storage, or distribution of Personal Information, the CEO or CTO or designee will:

1. Request a written statement from the customer (if not already captured in the contract) authorizing the disclosure of personal information to the third party for the intended purpose. The request will be documented and will be filed along with the evidence in the appropriate location.

2. Request a written statement from the third party to ensure that the third party complies with HIPAA or provides an equivalent level of privacy protection. The request will be documented and will be filed along with the evidence in the appropriate location.

All contracts shall specify that the customer/client and third parties can contact VPG via email or phone regarding inquiries or complaints about VPG's use of Personal Information. If the contract does not allow the inclusion of this statement, then the CEO or CTO or designee send the customer/client a separate letter or e-mail containing this statement. The recipient must acknowledge its receipt.

6.4. Assurance of Compliance

The CEO or CTO or designee will ensure that the adherence to the HIPAA and Privacy SOP and the protection of Personal Information is discussed as needed and trained on by all employees at least once every two years. If employees do not comply, appropriate actions shall be taken, which may include termination.

6.5. Escalation and Reporting of Potential and/or Accidental Breaches

If a breach of Personal Information protection occurs:

1. The employee/customer/site/subject/patient/user who became aware of such breach will notify the CEO or CTO or designee. Once notified, the CEO/CTO/designee will take measures to address the breach and involve resources as needed.

2. If VPG:
   a. Sent the information, the CEO or CTO or designee or the Security Council or designee:

      - Notifies the affected parties that a breach occurred.
      - Requests from the unintended recipients of such information the removal and/or destruction of this Personal Information.
      - Verifies the removal and/or destruction of this Personal Information.
      - Notifies the affected parties of such removal or destruction.

   b. Received the information, the CEO or CTO or designee:

- Notifies the sender of what unauthorized Personal Information was received, destroys the information, and confirms that it has been destroyed.
- Requests that the sender exercise due care in avoiding such transmissions in the future.

2. The CEO or CTO or designee documents the action taken and assesses if further investigation is needed.

7. Document History

Date	Version	Changes
04/23/2019	1.0	Initial procedure.

8. Document Approval

Jean-Philippe Couderc
Chief Executive Officer

Date

Gill Tsouri
Chief Technology Officer

Date