AVEGA
LEADING EDGE HEALTHCARE SOLUTIONS

DATA PRIVACY AND SECURITY MANUAL

By: Enterprise Risk Management and Compliance Department

Document Edit History

Version	Date	Additions/Modifications
0.1	Jun 18, 2014	Original
0.2	Dec 9, 2015	Revisions on policy for physical, computerized, and digital data
0.3	Apr 13, 2016	Added Data Privacy, Social Media, and Exception procedure policy
0.4	May 17, 2017	Revisions on data privacy and social media policy
0.5	Jun 26, 2018	Revisions and additions to the data privacy policy
0.6	Jan 25, 2019	Revisions on data privacy and exception procedure policy
0.7	Sep 5, 2019	DPO and COP functions were described. Replaced the Data Privacy and Security Committee.
0.8	Mar 31, 2020	Added related policies. Social Media Policy to be a standalone policy.
0.9	Oct. 13, 2020	Added Data Subject Rights and Revised Retention Policies. Data Retention Schedule to be attached.

Reviews and Approvals

Name	Function
Patrick Mitchell B. Sarmiento	Compliance Officer
Atty. Michael Balbanero	Senior Legal Counsel

1. Introduction

1.1. Objectives

The following are the purpose of this Manual, but not limited to:

1. To create and maintain an environment that safeguards data from threats to personal, professional, and institutional interests and to establish a comprehensive data security program in compliance with applicable law such as the Data Privacy Act of 2012 (Republic Act 10173).
2. To establish processes for ensuring the security and confidentiality of information.
3. To establish administrative, technical, and physical safeguards to protect against unauthorized access or use of information.
4. To establish, maintain, and promote data protection and a secured online presence that will:
   (1) protect the Company's physical and electronic data and IT systems;
   (2) build customers' trust and confidence; and
   (3) support the efficient processing of the Company's transactions and meet customers' needs.

1.2. Manual Owner

Enterprise Risk Management and Compliance Department (ERMCD).

1.3. Approval Authority

Any amendments to this policy have to be approved by the Board of Directors (BOD)

2. Data Protection Officer and Compliance Officers for Privacy

The Company adheres to the requirements of the Law (Republic Act 10173 or the Data Privacy Act of 2012) and the National Privacy Commission (NPC). It has appointed a Data Protection Officer (DPO) and several Compliance Officers for Privacy (COP). The DPO is a member of the Management Committee (ManComm) and likewise reports to the Executive Committee for the latest updates. Moreover, the DPO reports to the Risk Board Committee to appraise the Body of issues and developments concerning Data Privacy and Security.

Responsibilities of the Data Protection Officer (DPO)

1. Represent the organization in the event of an inquiry, inspection, or investigation by the National Privacy Commission.
2. Respond promptly to complaints or inquiries from data subjects.
3. Monitor the Organization's compliance with the DPA, its IRR, issuances by the NPC, and other applicable laws and policies.
4. Maintain confidentiality concerning the performance of his/her tasks.
5. Keep up-to-date on relevant privacy issues and appropriate data protection practices.
6. Lead the establishment and implementation of a Privacy Management Program, including continuous assessment and revision.
7. Coordinate with those who are responsible for related disciplines and functions within the Organization.
8. Be involved, properly, and promptly, in all issues which relate to privacy and data protection.
9. Advocate for personal data protection and privacy obligations within the Organization.

Consistent with the Advisory of the NPC, where a Company has branches, sub-offices, or any other component units, it may also appoint or designate a Compliance Officer for Privacy (COP) for each component unit. COP refers to an individual or individuals who shall perform some of the functions of a DPO. The DPO generally oversees the operations of the COP to ensure the performance of his/her functions, efficiently and economically, but without interfering with day-to-day activities.

The COP should actively coordinate and consult with the supervising DPO and should take instructions from the same. The following departments/groups will have COPs:

a. Human Capital Management and Development
b. Information Technology
c. Legal
d. Internal Audit
e. Medical Relations
f. Customer Service
g. Accounts Management
h. Operations
i. Regions

The amount of success the DPO and the COPs can achieve largely depends on the support given by several players and groups within the Organization:

Senior Management (Executive Committee)

- Budget support for security controls (technical, organizational, physical)
- Incorporating compliance into the performance bonus parameters of those concerned, especially for those handling personal data
- Drive the message throughout the organization
- Drive the urgency

Group and Line Heads

- Own/maintain their respective privacy impact assessments
- Consult on strategic projects involving the use of personal data ("privacy by design")
- Conduct breach drill regularly – test each privacy impact at least once a year

Human Capital Management and Development

- Roll-out training on privacy and data protection
- Issue security clearances to staff processing personal data (such clearance to be made contingent on passing the privacy training). DPOs must have access to all security clearances issued.
- Implement the recommended organizational controls

Legal

- Ensure that all PIP/service provider contracts, job orders, etc. are compliant with the DPA.
- Ensure that all external sharing of data meets the required guidelines of the NPC.

Other Support Functions

- Information Technology (IT) to implement the recommended technical controls
- Facilities and Property Administration (FPAD) to implement the recommended physical controls
- Internal Audit (IA) to test internally for compliance

3. Data Privacy Policy

This Policy provides for the standard procedure of Avega Managed Care, Inc. (the "Company") on the access, collection, use, and processing of all Personal Data, as defined herein, handled by the Company in the normal course of its business. Republic Act No. 10173 or the Philippine Data Privacy Act of 2012, as well as other pertinent laws and regulations on the privacy and security of data and information, are deemed integrated and read into this Policy. The objective of the Data Privacy Act is to protect the fundamental human right of privacy and communication while ensuring the free flow of information to promote innovation and growth. It also aims to ensure that Personal Data in information and communications systems in the government and the private sector are secured and protected.

Definition of Terms

- Controller refers to the Company and its contractors who participate in any form of Data Processing, as defined herein;

- Master Data Protection Agreement (MDPA)/Data Sharing Agreement (DSA) refers to the agreement that covers data sharing for commercial purposes, including direct marketing. The MDPA/DSA shall establish adequate safeguards for data privacy and security, and uphold the rights of data subjects. The agreement shall be subject to review by the Commission, on its initiative or upon complaint of the data subject;

- Data Subject refers to any individual (e.g., members and their beneficiaries, consultants or independent contractors) who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

- General Business Purpose refers to the purpose of the Company which is the management of health care needs of clients and, in the process, obtaining their data to provide a tailor-fitted healthcare program with the corresponding applicable premiums payable to Avega. Obtaining Personal Data is significant to the commercial operations of Avega, which include, but are not limited to sales, marketing, and research and development operations; protection of intellectual property; provision of services; internal operations; accounts management; information technology; and general employment matters, including both internal and external recruitment. Data retention and processing for General Business Purposes includes, but is not limited to, maintaining files, claims processing, managing benefit and healthcare plans for new and renewed accounts, conducting performance reviews, and intra-Avega communications.

- Personal Data is defined as any information related to an identified or an identifiable person which includes, but is not limited to, mailing address, phone number, email address, birth date, account number or family relationships, and gender.

- Processor is defined as an individual or entity engaged in processing Personal Data on behalf of the Controller, and/or under the Controller's control. A Processor may include, but is not limited to, the Legal, Human Resources, Claims Processing, Accounts Management, Sales and Marketing, Operations, and Finance and Accounting Departments of Avega. Avega requires Processors to protect the privacy, confidentiality, and security of Personal Data.

- Processing is defined as any operation or set of operations which are performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

- Sensitive Data is defined as a subset of Personal Data, and refers to any Personal Data on the following:

    - Payment information: billing history, insurance coverage, and, in some cases, credit card number

    - Health-related information: medical history and conditions, medication allergies, family's medical history, office visits, lab results, diagnoses, X-rays and other types of images, referrals to other medical professionals, prescriptions, lifestyle details (such as smoking and alcohol use), and other provider notes

- Third-Party is defined as any natural or legal person, public authority, agency, or any other entity other than the Data Subject, the Controller, the Processor, and the persons who, under the direct authority of the Controller or the Processor, are authorized to process the Personal Data.

Privacy Components

Privacy policies are documented (in writing) and made readily available to internal personnel and third parties who need them. Avega defines and documents its privacy policies for the following:

a. Notice
b. Choice and Consent
c. Collection
d. Use and Retention
e. Access
f. Disclosure to Third Parties
g. Security for Privacy
h. Quality
i. Monitoring and Enforcement

Communications

Privacy policies and the consequences of non-compliance with such policies are communicated at least annually to Avega internal personnel responsible for collecting, using, retaining, and disclosing PD (Personal Data), or PHI (Protected Health Information). Periodically communicates to internal personnel (for example, via SharePoint or memorandum) relevant information about privacy policies and changes. Avega requires internal personnel to confirm (initially and periodically) their understanding of an agreement to comply with Avega's privacy policies. Educates and trains internal personnel (initially and periodically) who have access to PD, PHI, or are charged with the security of PD, or PHI about privacy awareness, concepts, and issues. Changes in privacy policies are communicated to such personnel shortly after the changes are approved.

Responsibility

Responsibility and accountability are assigned to a person or group for documenting, implementing, enforcing, monitoring, and updating Avega's privacy policies. The names of such person or group and their responsibilities are communicated to internal personnel. Avega assigns responsibility for privacy policies to a designated person, i.e. the Data Protection Officer and the Compliance Officers for Privacy.

The authority and accountability of the designated person or group are documented. Responsibilities include:

a. Establishing standards to classify the sensitivity of PD and
b. To determine the level of protection required
c. Formulating, maintaining, monitoring, and updating Avega's privacy policies
d. Delegating authority for enforcing Avega's privacy policies
e. Monitoring the degree of compliance and initiating action to improve the training or clarification of policies and practices.

Avega requires users, management, and third parties to confirm (initially and annually) their understanding of and in agreement to comply with its privacy policies and procedures related to the security of PD and PHI.

Review and Related Policies

This Data Privacy Policy will be reviewed and/or amended every year to be consistent with the requirements of applicable law and the operations of the Company. Amendments will be approved by the Executive Committee and/or by the Risk Board Committee. This policy should be read together with, but not limited to:

- Information Security Policy
- Various IT Policies
    - Access Management Policy
    - Information Security Encryption Policy
    - Password Policy
    - Workplace Visitor Policy
    - Security Plan
- Privacy Policy
- Social Media Policy
- Data Breach and Security Incident Response Plan
- Relevant Memoranda and other business-specific policies relating to Privacy

Consistency of Privacy Policies and Procedures with Laws and Regulations

Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever there are changes to such laws and regulations. Privacy policies and procedures are revised to conform to the requirements of applicable laws and regulations. The Legal Department determines which privacy laws and regulations are applicable in the jurisdictions in which Avega operates and it reviews the privacy policies and procedures to ensure they are consistent with the applicable laws and regulations.

Infrastructure and Systems Management

Avega reviews the design, acquisition, implementation, configuration, and management of the infrastructure, systems, and procedures and changes thereto for consistency with Avega's privacy policies and procedures and address any inconsistencies.

Procedures are in place to:

a. Govern the development, acquisition, implementation, and maintenance of information systems and the related technology used to collect, use, retain, and disclose personal information.
b. Ensure that Avega's backup and disaster recovery planning processes are consistent with its privacy policies and procedures.
c. Classify the sensitivity of classes of data, and determine the classes of users who should have access to each class of data. Users are assigned user-access profiles based on their need for access and their functional responsibilities as they relate to personal information.
d. Assess planned changes to systems and procedures for their potential effect on privacy.
e. Test changes to system components to minimize the risk of an adverse effect on the systems that process personal information. All test data are anonymized.
f. Require the documentation and approval by the Data Protection Officer and the Responsibility Center Head before implementing the changes to systems and procedures that handle personal data, including those that may affect security. Emergency changes may be documented and approved on an after-the-fact basis.

The Information Technology (IT) department maintains a listing of all software and the respective level, version, and patches that have been applied. Procedures exist to provide that only authorized, tested, and documented changes are made to the system. Management reviews annually the assignment of personnel, budgets, and allocation of other resources to its privacy program.

Procedures

Use of Personal Data

In the course of the day-to-day business operations of the Company, its duly-authorized officers, staff, or persons otherwise designated according to Company procedure, may from time-to-time utilize and/or transfer Personal Data among various departments or offices of the Company provided that the utilization and transfer are necessary to carry out the Company's General Business Purposes. The Processing of Personal Data is allowed under the following circumstances:

a. There is written consent by the Data Subject. A written "authorization" (or written "consent") is required for any use or disclosure of the Data Subject's protected health information (or individually identifiable information) outside of legally permitted routine purposes (treatment, payment, health care operations) and other uses allowed or required by law. A valid authorization/consent form must include ***what*** can be shared, ***by and with whom***, for what ***purpose,*** and ***for how long***.
b. Necessary for the fulfillment of a contract or of a legal obligation;

c. In response to national emergency, public order and safety;
d. When the life and health, or other vital interests of the data subject are involved; or
e. In pursuit of legitimate interests by the personal information controller or by a third party to whom the data is disclosed provided that the fundamental rights and freedoms of the data are not violated.

Health records are considered Personal Data whether in paper or electronic copies.

Subject to the Company's compliance with the requirements for disclosure of Personal Data as required under the Data Privacy Act, subcontracting of the processing of Personal Data to any third party shall not relieve any person, department, or entity who subcontracts from full liability and accountability for ensuring compliance with the law and this policy (Sec. 14 of RA 10173).

Notice

The Company shall at all times inform Data Subjects of the purpose for which Personal Data shall be collected, used, processed, and stored. In certain situations, Personal Data may be presented or documented to remove any identification with the Data Subject, in which case such Personal Data becomes random or anonymous statistic or figure. In these cases, Data Subjects do not need to be notified.

The Data Subject has the right to know if their personal information is being processed. The Data Subject has the right to know information on said processing such as the source of the information, how their personal information is being used, and a copy of their information. One has the right to request removal and destruction of one's data unless there is a legal obligation on the part of Avega to keep or process such information. (Secs. 16 and 18 of RA 10173)

If the Data Subject has already passed away or has become incapacitated (for one reason or another), their legal assignees or lawful heirs may invoke said person's data privacy rights. (Sec. 17 of RA 10173)

Choice and Consent

Avega describes the choices available to the individual and obtains implicit or explicit consent for the collection, use, and disclosure of PD or PHI.

Data Subjects are informed about the choices available to them concerning the collection, use, and disclosure of personal information and that implicit or explicit consent is required to collect, use, and disclose personal information unless a law or regulation specifically requires otherwise.

Avega's privacy notice describes, in a clear and concise manner the choices available to the individual regarding the collection, use, and disclosure of personal information, the process an individual should follow to exercise these choices, and the consequences of failing to provide personal data.

Individuals are advised that personal data not essential to the purposes identified in the privacy notice need not be provided and that preferences may be changed and consent may be withdrawn at a later time, subject to legal or contractual restrictions and reasonable notice.

Consequences of withholding consent

When personal data is collected, individuals are informed of the consequences of refusing to provide personal information or of denying or withdrawing consent to use personal information for purposes identified in the notice. Avega informs individuals at the time of collection:

a. About the consequences of refusing to provide personal information (For example, transactions may not be processed.)
b. About the consequences of denying or withdrawing consent.
c. About how they will or will not be affected by failing to provide more than the minimum required personal information (For example, services or products will still be provided.)

Consent for New Purposes

If the information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the individual is notified and explicit consent is obtained before such new use or purpose. When personal information is to be used for a purpose not previously specified, Avega:

a. Notifies the individual and documents the new purpose.
b. Obtains and documents consent or withdrawal of consent to use the personal information for the new purpose.
c. Ensures that personal information is being used under the new purpose or, if consent was withdrawn, not so used.

Collection

Avega collects PDI and PHI only for the purposes identified in the notice. Individuals are informed that personal information is collected only for the purposes identified in the notice. Our privacy notice discloses the types of personal information collected and the methods used to collect personal information.

The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are documented and described in the privacy notice.

Collection Limited to Identified Purpose

The collection of personal information is limited to that necessary for the purposes identified in the notice. Systems and procedures are in place to:

a. Specify the personal information essential for the purposes identified in the notice and differentiate it from optional personal information.
b. Periodically review Avega's program or service needs for personal information (for example, once every five years or when there are changes to the program or service).
c. Obtain explicit consent when sensitive personal information is collected

d. Monitor that the collection of personal information is limited to that necessary for the purposes identified in the privacy notice and that all optional data is identified as such.

Collection by Fair and Lawful Means

Methods of collecting personal information are reviewed by management, Data Protection Officer, and legal counsel before they are implemented to confirm that personal information is obtained fairly, without intimidation or deception, and lawfully, adhering to all relevant rules of law relating to the collection of personal data.

Collection from Third Parties

Management and the Data Protection Officer confirms that third parties from whom personal data is collected (that is, sources other than the individual) are reliable sources that collect the information fairly and lawfully. Avega performs due diligence before establishing a relationship with a third-party data provider, reviews the privacy policies and collection methods of third parties before accepting personal information from third-party data sources. An MDPA/DSA is also required from third parties.

Use

Avega limits the use of PD to the purposes identified in the notice and for which the individual has provided explicit consent. Avega retains PD for only as long as necessary to fulfill the stated purposes.

Retention

Personal data is retained for no longer than necessary to fulfill the stated purposes unless a law or regulation specifically requires otherwise. Personal data no longer retained is disposed of and destroyed in a manner that prevents loss, misuse, or unauthorized access.

a. Documents its retention policies and disposal procedures.
b. Erases or destroy records per the retention policies, regardless of the method of storage (for example, electronic or paper-based).
c. Retains, stores, and disposes of archived and backup copies of records following its retention policies.
d. Ensures personal information is not kept beyond the standard retention time unless there is a justified business reason for doing so.
e. Locates and removes specified personal information about an individual as required, for example, removing credit card numbers after the transaction is complete.
f. Regularly and systematically destroys, erases, or makes anonymous personal information no longer required to fulfill the identified purposes or required by laws and regulations.

Access

Avega provides authorized individuals with controlled access to personal information for review and update. Individuals are informed about how they may obtain access to their personal information to review, update, and correct that information. Subject to exceptions allowed by law, Avega provides the data subjects all the means to update and correct personal data, including mechanisms to secure a portable copy of their data.

Disclosure to Third Parties

Avega discloses PD to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual. Moreover, a signed MDPA/DSA is required before data sharing. Avega's privacy policies address the disclosure of personal information to third parties.

Individuals are informed that personal information is disclosed to third parties only for the purposes identified in the notice and for which the individual has provided explicit consent unless a law or regulation specifically allows or requires otherwise. The disclosure includes any limitation on the third party's privacy practices and controls. Lack of such disclosure indicates that the third party's privacy practices and controls meet or exceed those of Avega.

Systems and procedures are in place to:

a. Prevent the disclosure of personal information to third parties unless an individual has given implicit or explicit consent for the disclosure.
b. Document the nature and extent of personal information disclosed to third parties.
c. Test whether a disclosure to third parties is in compliance with Avega's privacy policies and procedures, or as specifically allowed or required by law or regulation.
d. Document any third-party disclosures for legal reasons via a signed MDPA/DSA.

Personal information may be disclosed through various legal processes to law enforcement or regulatory agencies. Some laws and regulations have specific provisions for the disclosure of personal information. Some permit disclosure of personal information without consent while others require verifiable consent.

Personal information is disclosed only to third parties who have data sharing/protection agreements with Avega to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction and to ensure an adequate level of protection based on local and international standards.

Avega takes remedial action in response to misuse of personal information by a third party to whom Avega has transferred such information.

Security of Data

Avega takes reasonable precautions to protect Personal Data from loss, misuse, unauthorized access, disclosure, distribution, alteration, and destruction.

In the event such as Personal Data or the processing thereof is compromised, Avega must notify the affected data subjects and the National Privacy Commission, including other relevant privacy authorities, if applicable.

Information Security Program

Please see the Information Security Policy.

Transmitted Personal Information

Personal information is protected when transmitted by mail and over the Internet and public networks by moving towards the deployment of industry-standard encryption technology for transferring and receiving personal information.

Systems and procedures are being put in place to:

a. Address the confidentiality of information and communication and the appropriate protection of personal information transmitted over the Internet or other public networks.
b. Define minimum levels of encryption and controls.
c. Employ industry-standard encryption technology, for example, AES 128 bit transport layer security (TLS), for transferring and receiving personal information.
d. Approve of external network connections.
e. Protect personal information sent by mail, courier, or other physical means.

Quality

Avega maintains accurate, complete, and relevant PD for the purposes identified in the notice. Individuals are informed of their responsibility to Avega with accurate and complete personal information and for contacting Avega if the correction of such information is required. Avega privacy notice explains that the extent to which personal information is kept accurate and complete depends on the use of the information.

Enforcement

The Data Protection Officer, ERMC, and Legal will assure compliance with this Privacy Policy and periodically verifies that the policy is accurate, comprehensive for the information intended to be covered, prominently displayed, completely implemented and accessible and in conformity with the law. The Company encourages interested persons to raise any concerns to the DPO, causing the Company to investigate and resolve any complaints and disputes regarding the use and disclosure of Personal Data following the policy. The constitution of such a contact committee, as well as the formulation of procedures in investigating violations to this policy, shall constitute an amendment to and be deemed as part of this policy.

Rights of the Data Subject

Under RA 10173 or the Data Privacy Act of 2012, people whose personal information is collected, stored, and processed are called Data Subjects. Data subjects are given certain rights which they may request and require to the personal information controllers or processors, and which the latter are duty-bound to observe and respect.

The data subject can exercise their rights by sending a request to the Data Privacy Officer.

The right to be informed

- Before the collection of the personal data, through the consent form, data subjects are informed with basic information such as but is not limited to, the identity of the data controller, the purpose and the legal basis for processing the personal data, retention period and any other information necessary to ensure the fair and transparent processing of their data

The right to access

- The data subject has the right to request access to the personal data that Avega have processed. They have the right to obtain the following information:
  - The contents of the personal data that was processed
  - How the personal data was processed.
  - The recipients of the personal data
  - The reason for the disclosure of the personal data
  - The date when the personal data concerning the data subject were last accessed and modified
  - The designation, name or identity, and address of the personal information controller

The right to Correct/Rectify

- Avega ensures that all the personal data that it holds and uses the Data Subject is correct. If the personal data is not accurate the Data Subject has the right to require Avega to correct/rectify any inaccuracy or error in their data.

The right to Erasure/Blocking

- The data subject has the right to require Avega to suspend, withdraw, or order the blocking or removal of their data from the company's system. The data subject right may be exercised upon discovery and substantial proof of any of the following:
  - the personal data is incomplete, outdated, false, or unlawfully obtained
  - the personal data being used for a purpose not authorized by the data subject
  - the personal data is no longer necessary for the purposes for which they were collected
  - the data subject withdraws consent or object to the processing of their data and there is no other legal ground or overriding legitimate interest for the processing
  - The personal data concerns private information that is prejudicial to the data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
  - The processing is unlawful;
  - The personal information controller or personal information processor violated the rights of the data subject. The personal information controller may notify third parties who have previously received such processed personal information.

The right to object

- The data subject has the right to object any time to the processing of their data, including processing for direct marketing, automated processing, or profiling.

The right to data portability

- The data subject has the right to obtain an electronic copy of their data from the PIC.

Compliance Review

Compliance with privacy policies and procedures, commitments, and applicable laws, regulations, service level agreements, and other contracts are reviewed and documented and the results of such reviews are reported to management. If problems are identified, privacy policies and procedures are enforced.

4. Data Security Policy

The company must restrict access to confidential and sensitive data to protect it from being lost or compromised to avoid adversely impacting our members, incurring penalties for non-compliance, and suffering damage to our reputation. At the same time, we must ensure users can access data as required for them to work effectively. It is not anticipated that this policy can eliminate all malicious data theft. Rather, its primary objective is to increase user awareness and avoid accidental loss scenarios, so it touches on data classification, risk scenarios, and recommended data security measures on both physical and digital data.

Definition of Terms

- Company – Avega Managed Care, Inc., its subsidiaries, and affiliates
- Contact Information – This information is commonly available or distributed in public records and can be an individual's name, postal, or electronic mail address, telephone number.
- Data Destruction – Any action which prevents the recovery of information from the storage medium on which it is recorded (including encryption with unknown keys, erasure, reformatting, or disposal of the hardware needed to recover the information)
- Data Security Directives - These are issued by the Data Protection Officer to provide clarification of the Data Security Policy or to supplement the policy to more detailed procedures or specifications, or through action plans or timetables to aid in the implementation of specific security measures. All Data Security Directives issued by the DPO shall be deemed incorporated into the Data Privacy and Security Policy.
- Encryption Software – Custom or commercial software that encrypts data residing in a database, on disk, in the e-mail, or during transmission.
- Information Custodian – IT staff responsible for implementing and maintaining access controls and processes to protect data based on its classification level
- Information Owner – Functional group that initiates the creation of data and selects the appropriate classification level
- Information Resource - It is a discrete body of information created, collected, and stored in connection with the operation and management of the Company and used by its members having authorized access as a primary source. It includes electronic databases as well as physical files. Information derived from an Information Resource by authorized users is not an Information Resource, although such information shall be subject to Data Security Policy.
- IT Policies - It is a written set of technical standards and related procedures and protocols designed to protect against risks to the security and integrity of data that is processed, stored, transmitted, or disposed of through the use of the Company's information systems. It establishes minimum standards and may not reflect all technical standards and protocols in effect at any given time.
- Personally Identifiable Information (PD) - Any piece of data that, when combined with a person's Contact Information, uniquely identifies that individual and can be potentially used to access the individual's financial or personal resources.

PD can include the individual's social security number, date of birth, mother's maiden name, official state or country-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, government aid or food stamp account number, or bank account number, or credit or debit card number, including associated personal identification number or code (PIN) assigned to them; their unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; unique electronic identification number, address, or routing code; medical records, telecommunication identifying information or access device, or other unique number or information associated with that individual.

- Specific Security Procedures - These are procedures promulgated by Group Heads to address particular security needs of specific Information Resources sponsored within the area of responsibility, not otherwise addressed by the Data Security Policy or any Data Security Directives.
- Security Breach - It is an event that causes or is likely to cause Confidential Information to be accessed or used by an authorized person and shall include any incident in which the Avega is required to make a notification under the applicable law.
- Transportable Storage Media – USB thumb drives, external hard drives, internal hard drives which have been removed from a chassis, optical storage medium, floppy diskettes, solid-state storage of any kind, flash drives, smart cards, or any medium which can hold electronic data
- Users - These include virtually all officers and employees of the Company to the extent they have authorized access to company Information Resources and may include consultants, contractors, and temporary employees and volunteers.

Data Classification

All information covered will be classified according to the level of security required. These will be categorized as "Confidential", "Internal Use Only", or "Public".

a. Confidential information refers to the most critical and sensitive business and customer information that is intended strictly for use within Avega. Unauthorized disclosure of this type of data could seriously and adversely impact Avega, its customers, its business partners, and/or its suppliers.

   It includes sensitive personal and institutional information and must be given the highest level of protection against unauthorized access, modification or destruction. Unauthorized access to personal confidential information may result in a significant invasion of privacy or may expose the Company to significant financial risk. Unauthorized access or modification to institutional confidential information may result in direct, materially negative impacts on the finances, operations, reputation, or goodwill of the Company. Personal confidential information may include information protected under privacy laws, information concerning the pay and benefits of employees, personal identification information or medical/health information about Clients, and the data collected in the course of research. Institutional confidential information, on the other hand, may include Company's financial and planning information, legally privileged information, invention disclosures, and other information concerning pending patent applications, if any.

Without limiting the generality of the foregoing, confidential information shall include personal information, customer information, or any information that contains personally identifiable information that the Company obtains in the process of offering a product or service.

Passwords, encryption keys, PHI, and PD are considered a special class of confidential information that are subject to special controls.

b. Internal Use Only information includes information that is less sensitive than Confidential Information, but that, if exposed to unauthorized parties, may have an indirect or possible adverse impact on personal interests, or the finances, operations, or reputation of the Company. Examples of this type of data from an institutional or operational perspective include internal memos meant for limited circulation, or draft documents subject to internal comment before public release.

c. Public Information is generally available to the public, or that, if it were to become available to the public, would have no material adverse effect on individual members of the Company or upon the finances, operations, or reputation of Avega Managed Care, Inc. and its Clients.

d. Medical Information or Protected Health Information (PHI) means any individually identifiable information, whether oral or recorded in any form or medium, that:
   - is created or received by a healthcare provider, and benefit plan,
   - relates to past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past present or future payment for the provision of health care to an individual; and
   - Includes demographic data that permits identification of the individual or could reasonably be used to identify the individual.

All information resources, whether physical documents, electronic databases, or other collections of information, are to be assigned to a security classification level according to the most sensitive content contained therein.

In the event information is not explicitly classified, it is to be treated as follows:

a. Confidential if the data includes any personal information related to the operations of the Company including any health information, financial information, or other personal identification information.
b. Internal Use Only if the information is not classified as confidential unless such information appears in a form accessible to the public (i.e., on a public website or a widely distributed publication) or is created for a public purpose.

The Data Protection Officer may provide clarifications relating to the security classifications, and may, through the issuance of Data Privacy and Security Directives establish more detailed requirements concerning the classification of Information Resources or specific data.

5. Data Security Policy on Physical Data

Part of protecting our business is to make sure that confidential physical data must be safeguarded from any unauthorized access or use. The following data are considered private and confidential in our conduct of business, but not limited to:

1. Contracts
2. Members list and data
3. Client's benefit package
4. Internal financial reports
5. Internal Memos
6. Planning reports
7. Research data
8. Utilization record/medical record
9. Payment history and related Statement of Accounts, Official Receipts, and Credit Memos
10. HCMD records
11. Doctor's Records
12. Proposals
13. Franchising documents
14. Underwriting documents/commission arrangement
15. Minutes of meetings (Board, ExComm & ManComm)
16. Operating Manuals
17. Legal documents
18. Other management reports

Storage

- Documents shall be stored in locked cabinets. The storage area shall be provided for each department whose access will be limited to assigned personnel of the department only.
- The Company may also provide for secured off-site storage location outside its premises like bank vaults and a warehouse manned by a security guard.

Access

- All Confidential data must be protected via access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.
- Access to rooms containing confidential information shall always be recorded in a logbook or any through any means of recording data.
- Access to storage rooms exceeding the Employee's authorized classification level must be approved under the Exception Procedure Policy.

Transport

- Documents that may require transport should always be secured and sealed before transport.
- Storage boxes should bear proper labels.
- Bulk transport of documents from the premises to an off-site storage facility should only be done by Company employees using the Company vehicle.

- The transport should be authorized by a gate pass signed by a responsible officer and inspected by guards on duty from the site of source and site of destination.

Retention

The general retention period shall be 5 years following the Generally Accepted Accounting Practice (GAAP), except for documents subject to a prospective or pending legal case or claim for or against Avega, in which case the period may be longer than five years and provided the same is permitted by law. For medical information, the retention period shall be 10 years according to the Privacy Guidelines for the Implementation of the Philippine Health Information Exchange. Please refer to the below Data Retention Schedule specifying the prescribed periods of retention depending on the classification of documents.

Document	Retention Period	Medium	Location
HR Related Documents such as CVs, job application, notes taken during candidate interviews, test results, pre-employment background including criminal records and job references	While employment continues and 3 years from the date of last entry as prescribed by the Implementing Rules and Regulation of the Labor Code.	Electronic or paper Form	Makati City and Regional Offices, including warehouses
all books, registers, records, vouchers, and other supporting papers and documents prescribed by the BIR	10 years	For the first 5 years, physical copies are kept Electronic copies are also kept for 10 years	Makati City and Regional Offices, including warehouses
Documents containing medical Information	Subject to existing regulations, all medical records shall be stored for 15 years as prescribed by the DOH. Shorter periods shall be on a case by case basis and must be anchored on a rule issued by a proper government agency such as the NPC.	Paper and Electronic Form	Metro Manila (Head Office and warehouses upon archiving)
Documents not mentioned above	5 years following the general retention period prescribed by this Policy	Paper and Electronic Form	Metro Manila and the Regional Offices, including warehouses

Disposal

All Confidential and Internal Use Only documents for disposal should be shredded before disposal. Public documents may be used for recycling purposes but should ultimately be shredded before disposal.

Sanctions

Violations of the abovementioned policies are covered in the Code of Discipline (CoD).

Commented [AAA1]: Deleted specific reference to CoD as the same may be changed

6. Data Security Policy on Computerized and Digitized Information

All computerized and digitized information stored in the servers and any company-owned devices is subject to this Policy and the Information Security Policy.

Risk Identification

To protect our computerized and digitized data, we need to identify the security risks associated with this kind of information. Protection may come in:

(1) Protection related to data processing
(2) Protection related to theft, malicious destruction, corruption of hardware, and software.

The protection of data related to data processing will be covered by programs and software routines based on existing various IT and Information Security Policy. These policies are constantly reviewed and updated by the IT team and ERMC.

Protection of theft, malicious destruction, corruption of hardware, and software shall be covered by Data Security Policy.

The following are the most common security risks related to computerized and digitized data but not limited to:

- Hacking
  It is the use of malware (malicious software that is intended to damage or disable computers and computer systems) to remotely control, steal data, and destroy data, and corrupt hardware and software.

- Viruses
  These are malware programs that, when executed, replicates by inserting copies of itself into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be “infected”. It often performs some type of harmful activity on infected hosts such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their keystrokes.

- Cookies
  These are simple text files that are stored in a user’s machine by a web server. The text file contains information in a name-value pair, which can be retrieved by a website. This will track your website visits and can build a profile of your online interests and buying habits, and report these details to third parties.

- Phishing
  It is an attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in electronic communication. It usually uses fraudulent emails claiming to be from a trusted sender to “fish” for information.

- Pharming
  It is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent web sites without their knowledge or consent. Pharming has been called "phishing without a lure."

- Online Scam
  It uses internet services or software with internet access to defraud victims or to otherwise take advantage of them, for example by stealing personal information, which can even lead to identity theft.

- Social Engineering
  The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

To address the above-enumerated risks, the following shall be instituted, monitored, and controlled by the Company:

1) Firewalls subscription shall at all times be up to date and devices installed in all computerized and digitized sites of the Company. A continuous subscription gives an updated version of the firewall.
2) An anti-virus subscription shall at all times be activated and updated.
3) Browser settings upon installation as preferably using Chrome or Firefox.
4) Secured Socket Layer (SSL) should be enabled at all times for both e-mail systems and websites.
5) Removal of Command Prompt program or similar programs in company-issued computers and laptops.
6) Penetration and Vulnerability testing of systems at least once a year. Requiring third-party providers to undertake penetration and vulnerability testing of systems used by the Company.
7) Implement a proper back-up strategy and recovery plan to protect our business Information.
8) Train and inform stakeholders on proper disclosure of personal information.

Access Control

1) All Confidential data must be protected via access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.
2) Access to passwords, encryption keys, and PD must be encrypted, following the Encryption Policy and tracked, identifying who accessed it and when it was accessed.
3) Access to systems or applications handling Confidential information requires approval by the respective Department Head by the Exception Procedure Policy.
4) Access to data exceeding the Employee's authorized classification level must be approved following the Exception Procedure Policy.
5) Employees who have been authorized to view information at a particular classification level will only be permitted to access information at that level or a lower level.
6) Payment Card Industry data, including credit card Primary Account Number will be masked when displaying cardholder data, except for those individuals with a specific and legitimate need to see full credit card numbers.

7) Copying, moving, or storage of cardholder data onto local hard drives or other removable media is prohibited for personnel accessing cardholder data via remote-access technologies.
8) Avega will enforce access control through the use of centrally administered systems with modification to access rights logged accordingly.
9) Information owners will review and approve requests for access in line with the following requirements:
    a. Clear business needs.
    b. Awareness of information security policies and procedures.
    c. Awareness of incident reporting.
10) All parties accessing Avega information processing systems must utilize a unique account to link actions to an individual.
11) Built-in administration accounts shall not be used by an individual.
12) Redundant accounts will be regularly reviewed and disabled/removed.
13) All user accounts must be disabled when no longer used by an individual. Access rights must be revoked when no longer required to fulfill the business purpose, with regular review of assigned permissions.
14) Sessions used by individuals shall be restricted to a maximum idle-time to reduce the opportunity for unauthorized access. Systems will lock when maximum idle-time has been reached.
15) Applications used to facilitate information processing shall support unique accounts and least privilege permissions.

Password

1) Access to Avega information processing systems must be controlled by a combination of a username and password.
2) All default/vendor-supplied accounts will have their passwords changed before entering production.
3) Initial passwords will be changed upon first use.
4) Passwords shall be changed periodically with an immediate change required should any account be compromised.
5) Password complexity must be enforced, requiring minimum password length and a combination of alpha-numeric, upper/lower case, and special characters.

Mobile Equipment

1) Mobile computing devices must be secured when not in use to prevent loss or theft of the asset and information contained therein.
2) All mobile devices shall support and utilize password protection and encryption of sensitive data to prevent data loss in the event of theft.
3) Only the authorized individual is permitted to use a mobile device assigned to them, and only for business purposes.
4) Portable computers must not be left in view when unattended in public places or hotels.

Emails

1) All inbound external electronic mail (email) must pass through a mail relay that scans for inappropriate content and viruses.
2) All outbound emails must be scanned for viruses.
3) Avega reserves the right to monitor email to detect misuse.
4) Place mechanisms to detect and filter malicious email content and floods of unwanted messages are received.
5) Email users must adhere to Avega acceptable usage and Technology Assets Agreement which contain principles for the use of Avega Technology.

Internet

1) All inbound external Internet traffic must pass through a stateful firewall configured per Avega firewall policy and network-level intrusion detection system, to prevent unauthorized traffic and scan for inappropriate and malicious content.
2) Avega reserves the right to monitor Internet connectivity to detect misuse.
3) Internet users must adhere to Avega acceptable usage and Technology Assets Agreement which contain principles for the use of Avega technology. Access to the Internet for private use is permitted following these documents.

Back-Up System

1) Backups of important business data held on local servers must be taken at regular intervals and configured according to the system backup policy and associated documentation.
2) The backup system must verify the backup process was successful to ensure they can be restored correctly. Where appropriate data restored to key systems must be tested through a formal procedure.
3) Backups must always be taken before any major system changes.
4) Backup arrangements for individual systems shall also meet the requirements of the disaster recovery and business continuity policy and any associated plans.

System Monitoring and Vulnerability

1) System Monitoring & Vulnerability Scanning - The purpose of System Monitoring is to ensure that IT security controls are in place, effective, and identify security vulnerabilities to minimize potential impact.
2) Systems, servers, and network infrastructure components shall be configured to Avega build standards for system hardening.
3) Network and host-based intrusion detection systems/software shall be deployed to monitor for key events to indicate and alert upon malicious activity.
4) Vulnerability scans are conducted per Avega process and schedule as defined in the relevant documentation, with remediation of any identified vulnerabilities performed within the appropriate timeframe based on severity.

Sanctions

Violations of the abovementioned policies are covered by Sections 16 and 17 of the Code of Discipline (CoD). The following table of offenses will be used for reference #25, #26, and #30. Please see the Code of Discipline.

7. Policy Exceptions

Security Policy Exceptions

Avega Managed Care, Inc.'s (the "Company") Data Privacy and Security Policy institutes control for the protection of the Company's data and IT resources. As every exception to a policy or standard tends to weaken the protection of company IT Resources and underlying data, exceptions put in place will be strictly interpreted and applied only when legally allowed and justifiable. All employees who are responsible for ensuring appropriate enforcement of the Company's Data Privacy and Security Policy, and related standards governing company IT resources must comply with this Policy when requesting an exception to the Company's privacy and security policies, standards, guidelines, and procedures.

Procedure

The following procedure defines the process for the review and approval of exceptions to the Company's Data Privacy and Security Policy:

A manager (or his or her representative designated in writing) seeking an exception must assess the risks that the non-compliance may cause to the Company's IT resources and business processes. The Risk Management Framework can be used as a basis for coming up with a risk score and gauging the amount of acceptable risk. The Enterprise Risk Management team can assist in this phase.

Generally, exceptions to compliance can be justified only when compliance adversely affects business objectives or when the cost to comply offsets the risk of non-compliance. Nonetheless, any decision on granting exceptions to compliance shall be made on a case to case basis.
The risk analysis should include, but will not be limited to, identification of the threats and vulnerabilities in each situation, the likeliness of threats materializing or occurring, and the potential costs of an occurrence. Other matters that must be considered are the following:

1) What is the business reason for not complying with the information security policy or standard?
2) What is the information life cycle of the process, including backup and destruction of company data?
3) How will the process be hosted?
4) If a vendor is involved, what security controls does the vendor attest to?
5) What anti-malware is used?
6) What risk mitigation strategies are being considered?

Request for Exception Form

The Manager or his or her designee will submit a Request for Exception form to the Data Protection Officer (DPO), or his or her designee. The DPO and/or the Risk Officer will gather any necessary background information and make a recommendation to the ManComm. Also, the DPO may recommend that other departments review certain recommendations.

The ManComm shall act upon the request for an exception.

The requesting manager will be notified in writing of the decision of the ManComm.

All requests for exception will be retained by the DPO, Risk Officer, and/or the Management Committee.

Exceptions are valid for one year unless otherwise specified. Annually, the DPO will send a copy of approved exceptions back to the requesting manager who must determine whether the conditions that justified the original exceptions are still in effect and must report the determination to the ManComm thereafter. If the conditions have substantially changed, and an exception for compliance is still required, a new request must be submitted. Where there has been little to no change in circumstances, the period for the review process may be shortened as recommended by the Chairman of ManComm, his or her designee, and/or the Data Protection Officer.