Valley Medical Group

Annual WISP Review Checklist

Since your WISP was last reviewed have any of the following occurred:

- Has there been any reason to believe that a security breach occurred?
- Has there been a material change in the way in which your business functions? (i.e. moved, opened new location, added different services, etc.)
- Has the amount of Personal Information that you retain changed drastically?
- Has the type of Personal Information that you retain changed?
- Is there reason to believe that improved security measures are necessary at your business?

Review each section below. If changes are not required initial on the line below.

Introduction

Valley Medical Group (hereinafter referred to as "Company") has developed the following written information security plan with the objective of effectively administering and monitoring the protection of Personal Information that the Company owns or possess per the requirements of the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR 17.00. This plan addresses all aspects of maintaining security for Personal Information both electronically and physically. Our goal through this plan is to promote awareness throughout the Company of the importance of protecting personal information as well as to continually assess the security and confidentiality of the information we possess. This plan is broken down into the following parts: Administration, Protective Measures, and Post-Breach Actions.

The above section has been reviewed and requires no changes. (RR)

General Guidelines

The Company has the following general guidelines for the handling of Personal Information:

a) Be attuned to the Personal Information in your environment
b) Take reasonable steps to keep Personal Information secure and confidential. When not in use, Personal Information should be stored in its appropriate storage location. Electronic Personal Information should not be left open on a computer and when not in use, computers should be locked.
c) Avoid collecting Personal Information when it would serve no legitimate business purpose
d) Do not transport or send Personal Information outside of the Company whenever it can be avoided; and when it is absolutely necessary to transmit Personal Information, to ensure that appropriate security precautions are used to protect against loss, theft or unauthorized access.
e) Securely dispose of Personal Information when retaining it no longer serves a legitimate business purpose or is required by law.
f) If you become aware of a potential breach of security or the loss or theft of Personal Information, report it immediately to the Information Security Manager.

The above section has been reviewed and requires no changes. (RR)

Administration

Information Security Manager

The Company has designated an Information Security Manager, Raymond Rossini, who is charge of the following:

a) Developing, implementing, administering and maintaining this program and any policies and procedures necessary to effectuate this program
b) Assessing and identifying reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of Personal Information
c) Evaluating and improving, where necessary, the effectiveness of the program and the Company's safeguards for limiting risks to Personal Information.
d) Designing, implementing and overseeing ongoing employee training and awareness programs.
e) Managing and responding to incidents involving information security, such as breaches or potential breaches involving Personal Information or violations of this program.
f) Overseeing the Company's relationships and contracts with third party service providers to ensure the security of Personal Information.

The above section has been reviewed and requires no changes. (RR)

Training

The Company practices initial and periodic training of employees on the handling of Personal Information. This training includes information on what Personal Information is and the policies and guidelines that the Company has adopted with respect to the safekeeping of Personal Information. Employees are tested at the conclusion of such training to ensure that they fully understand the law and what is required of them to maintain the Company's compliance. Additionally, the Company takes reasonable steps to inform its information security policies to consultants and service providers who may have access to Personal Information.

The above section has been reviewed and requires no changes. (RR)

Monitoring and Review

The Information Security Manager works in conjunction with staff and administration in order to ensure that this plan is kept upto-date and followed. The Information Security Manager regularly monitors the company's compliance with this plan and works with the Company's administration, when necessary, to revise or change this document. A comprehensive review of this security plan is carried out at least annually as well as whenever there is a material change in the nature of the Company's business.

The above section has been reviewed and requires no changes. (RR)

Third Party Service Providers

Third party service providers as well as vendors and consultants who have access to the Company's personal information and/or to Personal Information of the Company's clients or employees are required to follow the same guidelines as all employees of the Company. The Company takes the following steps when working with third party service providers in order to maintain the safety of the Personal Information which we possess:

a) Before engaging a service provider who may have access to Personal Information, the Company shall conduct reasonable due diligence to assess whether the service provider is capable of maintaining appropriate security measures to protect Personal Information.
b) Upon engagement by the Company, any service provider who may have access to Personal Information should be made aware of this Program and the Company's information security policies and procedures.

c) The Company will also satisfy the need for due diligence by obtaining written representations that the service provider is in compliance with the Company's policies regarding the safeguarding of Personal Information.
d) The ISM shall periodically review the performance of service providers who have access to Personal Information to ensure that the service providers have put in place and maintained adequate security measures.

The above section has been reviewed and requires no changes. (RR)

Violations and Discipline

Violations of this Plan, including careless, accidental or intentional disclosures of Personal Information may result in disciplinary action, up to and including immediate termination of employment or all existing business relationships with the Company. Violators may also be subject to civil or criminal liability. The Company will evaluate the appropriate disciplinary measures and legal actions on a case-by-case basis.

The above section has been reviewed and requires no changes. (RR)

Protective Measures

Physical Security Measures

Access to Personal Information

Physical access to Personal Information and the Company's offices, files and computer systems is restricted to authorized individuals. The Company maintains a number of physical security precautions to ensure that physical access to Personal Information is limited to authorized individuals including:

- Server room with locked access for which only the ISM has possession of the key.
- Interior of building is protected with alarm system with keypad entry, motion sensors, door alarm, surveillance cameras and locked doors. Exterior of building is monitored with surveillance cameras of back parking lot.
- All keys are surrendered, personal alarm codes are deactivated and door locks are changed upon employee termination.
  - Documents including receipts containing customer payment information is kept in a locked storage area until shredded.

The above section has been reviewed and requires no changes. (RR)

Maintaining a Confidential Work Environment

Everyone is trained to use good judgment to make sure that Personal Information is secure. Employees are taught to avoid discussing Personal Information where it can be overheard by unauthorized individuals, such as in lobbies or other public areas. Papers, documents, computers and storage devices containing Personal Information are not left unattended in public areas, including in conference rooms, at copy machines, in automobiles, or at any locations outside of the office. When employees are away from their work area for an extended period of time, Personal Information is stored in locked cabinets, drawers or containers and computer screens are locked.

The above section has been reviewed and requires no changes. (RR)

Secure Disposal of Personal Information

When disposing of Personal Information, physical documents are redacted or shredded so that the Personal Information cannot be practicably read or recovered. Similarly, electronic files and any disk or device containing Personal Information is securely disposed of to prevent recovery of the Personal Information.

The above section has been reviewed and requires no changes. (RR)

Departing Employees and Service Providers

All employees, consultants and service providers must return and, upon request, destroy all Personal Information provided by the Company before their departure or earlier, upon the Company's request.

The above section has been reviewed and requires no changes. (RR)

Electronic Security Measures

Secure User Authentication

The Company has in place secure user authentication protocols, including (i) control of user IDs and other identifiers, (ii) a reasonably secure method of assigning and selecting passwords; and (iii) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect. The company assigns unique identifiers for access to computer systems in addition to passwords that are created by each individual user that must adhere to industry standard complexity requirements; passwords must be at least eight characters long, include both capital and lowercase letters, include at least one number, and include at least one symbol ($,%,^, etc.). Any device that remotely accesses email or file containing Personal Information will require MFA.

The above section has been reviewed and requires no changes. (RR)

The Company restricts access to authorized users and active user accounts only. These restrictions allow access to records and files containing Personal Information only to users with a need to access such Personal Information in order to perform their assigned job. The Information Security Manager determines in consultation with the Company's administration who shall be an authorized user with an active user account and which users need access to Personal Information in order to perform their job duties.

The above section has been reviewed and requires no changes. (RR)

The Company also requires that current computer or network passwords are changed periodically. The Company blocks access to users after multiple unsuccessful attempts to gain electronic access to computers or the network.

The above section has been reviewed and requires no changes. (RR)

Remote network access is granted via unique usernames and passwords over a secure network.

The above section has been reviewed and requires no changes. (RR)

Upon termination, former employees are promptly disabled within the Company's network which disallows access to all computers and network shares where Personal Information is stored.

The above section has been reviewed and requires no changes. (RR)

Encryption

All transmitted records and files containing Personal Information that will travel across public networks is securely encrypted. Any and all Personal Information to be transmitted wirelessly is encrypted. Additionally, all Personal Information stored on laptop computers or portable devices is encrypted

The above section has been reviewed and requires no changes. (RR)

Security Software

All computers connected to the Company's network are installed with reasonably up-to-date security software including firewall protection and virus/malware protection. Additionally, all computers are kept reasonably up-to-date with recent security system software patches.

The above section has been reviewed and requires no changes. (RR)

Post-Breach Actions

In the event of a security breach or a loss of Personal Information, all facts regarding this security breach are promptly and accurately relayed to the Information Security Manager. The Company also possesses a Security Breach form which shall be completed by either the party who became aware of the security breach or the Information Security Manager as deemed appropriate by the Information Security Manager. The Information Security Manager shall investigate and take prompt action (in conjunction with other administrators at the Company, if necessary) to prevent harm and avoid liability. The Information Security Manger will also provide a report documenting the incident and responsive actions taken or to be taken in connection with the incident. Based on the results of the Company's investigation, internal and/or external parties may be notified, as necessary and appropriate.

The above section has been reviewed and requires no changes. (RR)

Upon notification of a suspected Personal Information security breach the Information Security Manager will:

- Report the breach to the appropriate officials
- Block, mitigate, or de-escalate the breach, if possible.
- Implement processes and procedures to prevent similar breaches from occurring in the future.
- Take necessary action to notify parties affected and or state agencies when appropriate.

The above section has been reviewed and requires no changes. (RR)

Internal Notification

The Information Security Manager will report all suspected cases of significant information breaches to company management and will work with them to establish an appropriate response strategy. If the investigation into the security breach determines that criminal activity has taken place, the Information Security Manager (or designee) will report the breach to appropriate legal authorities and/or the police.

The above section has been reviewed and requires no changes. (RR)

External Notification

The Information Security Manager in consultation with company management will determine if external notification will be required in the event of an information breach. External notification is required if any of the following conditions are met:

- Access has been gained to Personal Information as defined in MA CMR 17
- A physical device that contains Personal Information has been lost or stolen
- There is evidence that unencrypted Personal Information has been copied or removed
- There is evidence that an intrusion was intended to acquire unencrypted Personal Information

The above section has been reviewed and requires no changes. (RR)

Parties to be notified may include:

- Anyone affected by the breach, or whose data may have been compromised.
- Government officials as required by law, such as the attorney general of Massachusetts.

The above section has been reviewed and requires no changes. (RR)

Valley Medical Group

Authorized Signature

Raymond Rossini
Printed Name

11/16/23
Date