TotalWellness

Information Security Policy

Last Update: October 23, 2023

TABLE OF CONTENTS

INTRODUCTION 4

Purpose 4
Scope 4
Applicable Statutes / Regulations 4
Privacy Officer 4

DEFINITIONS & CLASSIFICATIONS 5

Data Classification 5

EMPLOYEE RESPONSIBILITIES 7

Employee Requirements 7
Prohibited Activities 7
Electronic Communication, E-mail, Internet Usage 8
Internet Access 10
ANTI-VIRUS AND ANTI-MALWARE 10
NETWORK And application Security 10
MOnitoring Compliance 11
Reporting Software Malfunctions 11
Report Security Incidents 11
Transfer of Sensitive/Confidential Information 12
Transferring Software and Files between Home and Work 12
The use of email containing phi 12
Use of encrypted e-mail 13
Secure File Transfer Protocol (sftp) 13
Data Encryption 13
electronic Storage of Protected Information 14
Physical Storage of Protected Information 14
Data Loss Prevention (DLP) 14
TotalWellness utilizes the following mechanisms for Data Loss Prevention. 14
De-identification / Re-identification of Personal Health Information (phi) 14

IDENTIFICATION AND AUTHENTICATION 15

User Logon ids 15
Passwords 15
Confidentiality Agreement 16
Safeguarding phi & pii 16
Controlled Access 17
Termination of User Logon Account 17

BUILDING SECURITY 18

TELECOMMUTING 19

General Requirements 19
Hardware Security Protections 19
Data Security Protection 19
Mobile Devices 20

DISPOSAL OF PAPER & EXTERNAL MEDIA/HARDWARE 22

Disposal of Paper and/or External Media 22
Disposal of External Media 22
Requirements Regarding Equipment 23
Disposition of Excess Equipment 23

CONTINGENCY PLAN 24

Statement of Policy 24
Procedure 24

SECURITY AWARENESS AND TRAINING 26

Statement of Policy 26
Procedure 26

SECURITY MANAGEMENT PROCESS 28

Statement of Policy 28
Procedure 28

Introduction

PURPOSE

This policy defines the technical controls and security configurations users are required to implement in order to ensure the integrity of the data environment at Vaccination Services of America, Inc. d/b/a TotalWellness, hereinafter, referred to as TW. It serves as a central policy document with which all employees and contractors must be familiar, and defines actions and prohibitions that all users must follow. The policy provides guidelines concerning the acceptable use of TW technology equipment, e-mail, Internet connections, facsimile, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all TW employees or temporary workers at all locations and by contractors working with TW as subcontractors.

SCOPE

This policy document defines common security requirements for all TW personnel and systems that create, maintain, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of TW, entities in the private sector, in cases where TW has a legal, contractual or fiduciary duty to protect said resources while in TW custody. In the event of a conflict, the more restrictive measures apply. This policy covers TW network system which is comprised of various hardware, software, communication equipment and other devices designed to assist TW in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any TW domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by TW at its office locations or at remote locales.

APPLICABLE STATUTES / REGULATIONS

The following is a list of the various agencies/organizations whose laws, mandates, and regulations were incorporated into the various policy statements included in this document.

HIPAA Security Rule, including but not limited to 45 CFR 164.316

PRIVACY OFFICER

TW has established a Privacy Officer as required by HIPAA. This Privacy Officer will oversee all ongoing activities related to the development, implementation, and maintenance of TW privacy policies in accordance with applicable federal and state laws. The current Privacy Officer for TW is:

Alan Kohll

Definitions & Classifications

DATA CLASSIFICATION

In order to appropriately handle data, it is vital for employees to understand TotalWellness's classification of data.

Confidential or Sensitive Data Classification
This classification applies to information that is intended for use within TotalWellness. Its unauthorized disclosure could adversely impact TotalWellness or its customers, suppliers, business partners, employees or participants.

Confidential or Sensitive Data includes:

Protected Health Information (PHI)
Protected Health Information (PHI) is individually identifiable health information that relates to a past, present or future physical or mental health condition, health care for that condition and/or payment for that care.

PHI Includes:

- Service documentation (consent forms)
- Screening values/lab results
- Appointment dates/times
- Health history
- Participant Identifiers, when using in conjunction with health data

PHI includes information by which the identity of a participant can be determined with reasonable accuracy and speed either directly or by reference to other publicly available information.

Examples of Participant Identifiers:

- Names
- Social Security Numbers
- Birth Dates
- Telephone numbers
- Email addresses

PHI must be protected if collected, stored, or used by TotalWellness.

Personal Identifiable Information
Personal Identifiable Information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

PII Includes:

- Names
- Social Security Numbers
- Birth Dates
- Telephone numbers
- Email addresses

PII must be protected if collected, stored, or used by TotalWellness.

TotalWellness Business Information
TotalWellness Business Information includes information specific to TotalWellness such as client information, pricing, policies, systems, etc. TotalWellness Business Information must be protected if collected, stored, or used by TotalWellness.

Public Data Classification:
This classification applies to information that has been approved by TotalWellness management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm.

Public Data Includes:
- TotalWellness website content
- TotalWellness blog content
- TotalWellness Address
- TotalWellness Phone Number

Employee Responsibilities

EMPLOYEE REQUIREMENTS

The first line of defense in data security is the individual TW user. TW users are responsible for the security of all data, which may come to them in whatever format. TW is responsible for maintaining ongoing training programs to inform all users of these requirements.

Challenge Unrecognized Personnel **-** It is the responsibility of all TW personnel to take positive action to provide physical security. If you see an unrecognized person in a restricted TW office location, you should challenge them as to their right to be there. All visitors to TW offices must sign in at the front desk. All other personnel must be employees of TW. Any challenged person who does not respond appropriately should be immediately reported to supervisory staff.

Secure Laptop in Locked Drawer **-** When out of the office all laptop computers with PHI must be secured. Most TW computers will contain sensitive data either of a medical, personnel, or financial nature, and the utmost care should be taken to ensure that this data is not compromised.

Unattended Computers **-** Unattended computers should be locked by the user when leaving the work area. This feature is discussed with all employees during yearly security training. TW policy states that all computers will have the automatic screen lock function set to automatically activate upon ten (10) minutes of inactivity. Employees are not allowed to take any action that would override this setting.

Home Use of TW Corporate Assets - Only computer hardware and software owned by and installed by TW is permitted to be connected to or installed on TW equipment. Only software that has been approved for corporate use by TW may be installed on TW equipment. All employees and contractors must read and understand the list of prohibited activities that are outlined below. Modifications or configuration changes are not permitted on computers supplied by TW for home use.

Retention of Ownership - All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of TW are the property of TW unless covered by a contractual agreement. Nothing contained herein applies to software purchased by TW employees at their own expense.

Removable Media – Removable media such as CD's, DVD's, and USB drives are not to be used to store PHI or PII unless provided with authorization from the Security Officer. If authorization is provided all data stored on removable media must be encrypted. Employee may not take removable media off of TW property.

PROHIBITED ACTIVITIES

Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

- Crashing an information system. Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that

the crash occurred as a result of user action, a repetition of the action by that user may be viewed as a deliberate act.

- Attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.
- Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an information system.
    - Exception: Authorized information system support personnel, or others authorized by TW Privacy Officer, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.
- Browsing. The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. TW has access to patient level health information which is protected by HIPAA regulations which stipulate a "need to know" before approval is granted to view the information. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.
- Personal or Unauthorized Software. Use of personal software is prohibited. All software installed on TW computers must be approved by TW.
- Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by TW is strictly prohibited.
- System Use. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of TW is strictly prohibited.
- Pictures and Recordings. Taking pictures or recordings of TotalWellness confidential information is strictly prohibited. Employees with access to secure areas are not allowed to bring cell phones, cameras, or any external storage devices (IE. USB drives, external hard drives, voice recorders, etc.) into the secure areas.

ELECTRONIC COMMUNICATION, E-MAIL, INTERNET USAGE

As a productivity enhancement tool, TW encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by TW owned equipment are considered the property of TW – not the property of individual users. Consequently, this policy applies to all TW employees and contractors, and covers all electronic communications including, but not limited to, telephones, e-mail, voice mail, instant messaging, Internet, fax, personal computers, and servers.

TW provided resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, and Internet software and services are intended for business purposes and for use by authorized TW staff only. However, incidental personal use is permissible as long as:

1) it does not consume more than a trivial amount of employee time or resources,
2) it does not interfere with staff productivity,
3) it does not preempt any business activity,
4) it does not violate any of the following:

    a) Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or

videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.

b) Illegal activities – Use of TW information resources for or in support of illegal purposes as defined by federal, state or local law is strictly prohibited.
c) Commercial use – Use of TW information resources for personal or commercial profit is strictly prohibited.
d) Political Activities – All political activities are strictly prohibited on TW premises. TW encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using TW assets or resources.
e) Harassment – TW strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, TW prohibits the use of computers, e-mail, voice mail, instant messaging, texting and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.
f) Junk E-mail - All communications using IT resources shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.
g) Confidential Information. Employees may not utilize any personal accounts to transmit confidential TotalWellness information. Personal accounts include personal email, IM, VoIP, Text Message, and other external communications application.
h) Media Streaming. Employees may not stream media on their TW provided equipment or utilizing TW providing internet, unless the streaming media is directly related to their job function and approved in advance, IE. Training videos, wellness webinars, etc.

Generally, while it is **NOT** the policy of TW to monitor the content of any electronic communication, TW is responsible for servicing and protecting TW's equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals. For example, an audit or cost analysis may require reports that monitor phone numbers dialed, length of calls, number of calls to / from a specific handset, the time of day, etc. Other examples where electronic communications may be monitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems and detecting patterns of abuse or illegal activity.

TW reserves the right, at its discretion, to review any employee's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as TW policies. TW does not allow personal information and documents to be stored on TW equipment.

Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others. All TW emails should contain the following disclaimer.

> Disclaimer: This email and any files transmitted with it are confidential. If you have received this email in error please notify the sender and then delete it immediately.

INTERNET ACCESS

Internet access is provided for TW users and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. The Internet access provided by TW should not be used for entertainment, social media, listening to music, viewing the sports highlight of the day, games, movies, etc. Do not use the Internet as a radio or to constantly monitor the weather or stock market results. While seemingly trivial to a single user, the company wide use of these non-business sites consumes a huge amount of Internet bandwidth, which is therefore not available to responsible users.

Users must understand that individual Internet usage is monitored, and if an employee is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken.

ANTI-VIRUS AND ANTI-MALWARE

All TotalWellness systems (workstations, servers, etc.) are equipped with antivirus and antimalware prevention software – SentinelOne EDR client. Employee emails are protected with IronScales email security and Microsoft 365 Encryption. Employees are not authorized to disable or remove this software. Software update processes are completed weekly or immediately for critical updates.

NETWORK AND APPLICATION SECURITY

All TotalWellness networks are protected with industry best practice level firewalls. The firewalls maintain security logs. The firewalls are monitored and any indications that unauthorized security related activities have been attempted or performed on a system or application are investigated.

The network is secured behind a Fortinet FortiGate firewall with security service enabled. There is a web server on a DMZ network and a database server on a trusted network. The firewall only permits approved devices to connect to the internal network. The TotalWellness VPN is configured with two-factor authentication. The firewall utilizes IDS/IPS, web content filtering, and antivirus capabilities. Devices must be joined to the domain by DataServ staff for internal access through a standardized approval process.

Software patches are applied frequently, at a minimum weekly, with critical patches applied as soon as possible. The systems, firewall and servers, and reviewed and updated monthly, the third weekend of the month.

MONITORING COMPLIANCE

TotalWellness department managers are responsible for ensuring staff members on their team are abiding by the outlined privacy and security policies. If non-compliance is observed the instance is to be documented by the manager including the date, offending individual, offence, remediation plan, and disciplinary action. Logs are to be maintained by each department manager for a minimum of 3 years. If an individual has more than 3 offences in a 6 month time frame the department manager is to notify the Privacy Officer and disciplinary action may be taken against the offending employee.

The TotalWellness systems log read access and changes including the changed value and user who made the change. Access right changes are logged and logs are maintained for a minimum of 12 months. Network logs are recorded and maintained for a minimum of 12 months.

REPORTING SOFTWARE MALFUNCTIONS

Users should inform the appropriate TW personnel and DataServ when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection, TW computer virus policy should be followed, and these steps should be taken immediately:

- Stop using the computer
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.
- Inform the appropriate personnel as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected virus.
- The employee should monitor the resolution of the malfunction or incident, and report to the Security Officer the result of the action with recommendations on action steps to avert future similar occurrences.

REPORT SECURITY INCIDENTS

It is the responsibility of each TW employee or contractor to report perceived security incidents on a continuous basis to the appropriate supervisor or security person. A User is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security incidents or violations of the security policy immediately to the Privacy Officer. Users should report any perceived security incident to their immediate supervisor.

Reports of security incidents shall be escalated as quickly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents are logged and the remedial action indicated. It is the responsibility of TW to

provide training on any procedural changes that may be required as a result of the investigation of an incident.

Security breaches shall be promptly investigated. If criminal action is suspected, TW Privacy Officer shall contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police or the FBI.

Clients will be notified by TotalWellness of any suspected security incidents and/or application vulnerabilities. TotalWellness will provide written documentation articulating what the incident was, the cause of the incident, the steps taken to mitigate the incident and the remediation plan to prevent similar incidents form occurring in the future.

TRANSFER OF SENSITIVE/CONFIDENTIAL INFORMATION

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by TW and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of TW policy and will result in personnel action, and may result in legal action.

PHI and PII data are encrypted at rest and in transit. PHI and PII data will only be transferred upon client request to a third party using a secure transfer method. Client data will be transferred upon the frequency requested by the receiving third party. Client data will not be transferred to any other third party without the prior written consent of the client.

Upon request, TotalWellness will transfer participant past participation data of a terminated client to a third party using secure methods after receiving written approval from the client.

TRANSFERRING SOFTWARE AND FILES BETWEEN HOME AND WORK

Personal software shall not be used on TW computers or networks. If a need for specific software exists, submit a request to your supervisor. Users shall not use TW purchased software on home or on non-TW computers or equipment.

TW proprietary data, including but not limited to patient information, IT Systems information, financial information or human resource data, shall not be placed on any computer that is not the property of TW without written consent of the respective supervisor or department head. It is crucial to TW to protect all data and, in order to do that effectively we must control the systems in which it is contained. In the event that a supervisor receives a request to transfer TW data to a non-TW Computer System, the supervisor should notify the Privacy Officer or appropriate personnel of the intentions and the need for such a transfer of data.

THE USE OF EMAIL CONTAINING PHI

Sending Protected Health Information (PHI) by email exposes the PHI to two risks:

- The email could be sent to the wrong person, usually because of a typing mistake or selecting the wrong name in an auto-fill list.
- The email could be captured electronically en route.

HIPAA requires that we take reasonable steps to protect against these risks but acknowledges that a balance must be struck between the need to secure PHI and the need to ensure that providers can efficiently exchange important information.

Encrypting information when it's e-mailed helps to keep this information from being intercepted, viewed, or stolen by people who do not have a right to it.

“Personally identifiable information" means any information that identifies an individual or has the ability to identify an individual. A good rule of thumb is, if you're not sure if information you're e-mailing should be encrypted, encrypt it. When in doubt - Encrypt.

USE OF ENCRYPTED E-MAIL

All TW employee email accounts have the ability to send encrypted emails using Microsoft 365 encryption. To encrypt an email employees must be using Microsoft Outlook or Outlook Web Access. Type Encrypt in the subject line or body of an e-mail. You should not use quotes around the word encrypt and you should not use variations of the word encrypt (IE. Encryption, encrypted, etc.) It does not matter if you type ENCRYPT, Encrypt or encrypt. In other words, capitalization does not matter.

The recipient will automatically receive instructions on how to retrieve their encrypted message. These instructions include information on what to do if they experience problems.

SECURE FILE TRANSFER PROTOCOL (SFTP)

Files may be transferred to secure FTP sites through the use of appropriate security precautions.

DATA ENCRYPTION

At the application level data is encrypted using AES 256. TotalWellness uses Transparent Data Encryption (TDE) for SQL Server database encryption and Microsoft Windows Bitlocker for whole disk level encryption. When in transit, data is encrypted using TLS 1.2 and HTTPS.

Clients may opt for additional encryption on file transfers. When encrypted files are transferred between TotalWellness and an authorized third party the files are encrypted with a public key and signed with a private key. Both sides must hold the correct keys to decrypt the files. Encryption keys are only accessible by authorized individuals who have a need to access the keys. Expiration dates are included on keys and out of date keys are securely deleted. If a client no longer uses TotalWellness, any client specific keys are revoked. Keys are only shared via secure means such as SFTP.

ELECTRONIC STORAGE OF PROTECTED INFORMATION

All data files and images containing protected health information (PHI) or personal identifiable information (PII) are to be stored on the encrypted network server. Data should not be store on individual machines. Client data is separated by client and access is limited by user using access control. Within applications, each database is separate from each other based on the application. Each database has its own independent user account.

All data is backed up based using best practices. A backup is completed on premises through a multifactor authenticated NAS. A backup copy is also stored through the cloud using Storagecraft's data cloud backup. All backups are encrypted in transit and at rest using the same standards as original data storage.

PHYSICAL STORAGE OF PROTECTED INFORMATION

Physical forms containing PHI and/or PII are stored in an access controlled area within the TotalWellness facility. Access is limited to only those with a need to access the area. The storage area is equipped with key-card access, security cameras, and alarms.

DATA LOSS PREVENTION (DLP)

TotalWellness utilizes the following mechanisms for Data Loss Prevention.

- Remote access to data is handled on a case by case basis and must be approved by the Security Offices. Remote access is only given through a Group Policy controlled VPN connection which is authenticated through multifactor authentication.
- All data is backed up based off of best practices. A backup on premises through a multifactor authenticated NAS, and through the cloud using Storagecraft's data cloud backup. All backups are encrypted.
- Emailed information goes through Microsoft Office 365 defender which scans emails and sifts out all malicious email attacks and possible Phishing. All email accounts are protected through multifactor authentication.
- All computer profiles are saved through folder re-direction through one drive which is authenticated through multifactor authentication.

DE-IDENTIFICATION / RE-IDENTIFICATION OF PERSONAL HEALTH INFORMATION (PHI)

As directed by HIPAA, all personal identifying information is removed from all data that falls within the definition of PHI before it is stored or exchanged. De-identification is defined as the removal of any information that may be used to identify an individual.

PHI includes:

- Names
- Addresses
- Geographic subdivisions smaller than a state

- All elements of dates directly related to the individual (Dates of birth, marriage, death, etc.)
- Telephone numbers
- Facsimile numbers
- Email addresses
- Social security numbers
- Medical record numbers
- Biometric identifiers

Re-identification of confidential information: A cross-reference code or other means of record identification is used to re-identify data as long as the code is not derived from or related to information about the individual and cannot be translated to identify the individual. In addition, the code is not disclosed for any other purpose nor is the mechanism for re-identification disclosed.

Identification and Authentication

USER LOGON IDS

Individual users shall have unique logon IDs and passwords. An access control system shall identify each user and prevent unauthorized users from entering or using information resources. Security requirements for user identification include:

- Each user shall be assigned a unique identifier.
- Users shall be responsible for the use and misuse of their individual logon ID.

All user login IDs are audited at least twice yearly and all inactive logon IDs are revoked. TW Department Manager notifies the appropriate personnel upon the departure of all employees and contractors, at which time login IDs are revoked.

The logon ID is locked or revoked after a maximum of three (3) unsuccessful logon attempts which then require the passwords to be reset by the appropriate Administrator.

PASSWORDS

User Account Passwords
User IDs and passwords are required in order to gain access to all TW networks and workstations. All passwords are restricted by a corporate-wide password policy to be of a "Strong" nature. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. Users are required to select a password in order to obtain access to any electronic information both at the server level and at the workstation level. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

Password Length – Passwords are required to be a minimum of eight characters.

Content Requirements - Passwords must contain a combination of upper and lower case alphabetic characters, numeric characters, and special characters.

Change Frequency – Passwords must be changed every 60 days. Compromised passwords shall be changed immediately. Users are not allowed to change passwords more than once in a 24-hour period.

Reuse - The previous five passwords cannot be reused.

Lockout – Accounts will be locked out for 60 minutes after three failed password attempts.

Restrictions on Sharing Passwords - Passwords shall not be shared, written down on paper, or stored within a file or database on a workstation and must be kept confidential.

Restrictions on Recording Passwords - Passwords are masked or suppressed on all online screens, and are never printed or included in reports or logs. Passwords are stored in an encrypted format.

CONFIDENTIALITY AGREEMENT

Users of TW information resources shall sign, as a condition for employment, an appropriate confidentiality agreement. The agreement shall include the following statement, or a paraphrase of it:

> *I understand that any unauthorized use or disclosure of information residing on TW information resource systems may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.*

Temporary workers and third-party employees not already covered by a confidentiality agreement shall sign such a document prior to accessing TW information resources.

Confidentiality agreements shall be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending or employees are leaving an organization.

SAFEGUARDING PHI & PII

In order to maintain confidentiality, any item containing PHI and/or PII must follow the standards identified below.

- Employees must not leave any PHI and/or PPI on fax machines, printers, or copies.
- Employees are to clean their workspace of PHI and/or PII at the end of their work day. All PHI and PII must be securely locked up when unattended during the day and when the employee leaves for the day.
- Employees must exercise caution and discretion when leaving voicemail messages containing PHI and/or PII.
- Employees must verify participant identity by matching at least three data points (first name, last name, date of birth, unique ID, etc.) prior to providing or entering participant PHI and/or PII.

- Employees must position monitors to not be viewable by passersby or close off their area when working with PHI and/or PII.
- PHI and PII are encrypted at rest and in transit.
- PHI and PII data can only be transferred using security methods such as SFTP.
- Access to PHI and PII data utilizes the least privilege necessary methodology.
- Client data is separated by client and access to each client's data is limited using access control.

CONTROLLED ACCESS

TW provides employees with access to shared drives, long term storage, scan room, and applications based on employment level. Access is provided on a need to know basis, and TW limits the access to that employees have access to the least amount of information possible to complete their job functions. Access levels per department are outlined in the chart below

Department	Shared Drive Access	Operations Drive Access	Accounting Drive Access	Scheduler Access	Register My Time Access	Website Admin Access	Scan Room	Long Term Storage
Accounting	Yes	No	Yes	Limited	No	No	Yes	Yes
Account Management	Yes	Yes	No	Limited	Yes	Yes	No	Yes
Customer Support	Yes	No	No	Limited	Yes	Yes	No	No
Data	Yes	Yes	No	Limited	No	Yes	Yes	No
Recruitment	Yes	No	No	Limited	No	No	No	No
Scheduling	Yes	No	No	Limited	No	No	No	No
Shipping	Yes	No	No	Limited	No	No	No	No
Sales	Yes	No	No	Limited	Yes	No	No	No
Marketing	Yes	No	No	Limited	No	Yes	No	No
Field Operations	Yes	No	No	Limited	No	No	No	No
Reception	Yes	No	No	Limited	No	No	Yes	No
Operations	Yes	Yes	No	Yes	Yes	Yes	No	Yes

Privileged access and administrative access are only granted on an as needed basis and must be approved by the security officer. Each TotalWellness application has its own separate database and each database has its own independent user account. Users must have separate approved credentials to access each application.

TERMINATION OF USER LOGON ACCOUNT

Upon termination of an employee, whether voluntary or involuntary, employee's supervisor shall promptly notify IT Administrator. If employee's termination is voluntary and employee provides notice, employee's supervisor or department head shall promptly notify the IT Administrator of employee's last scheduled work day so that their user account(s) can be configured to expire. All accounts will expire within 30 minutes of the employee leaving the

premises. The employee's department head shall be responsible for insuring that all keys, ID badges, and other access devices as well as TW equipment and property is returned to TW prior to the employee leaving TW on their final day of employment.

Building Security

- Swipe cards control access to all building entrances. Attempted entrance without authorization results in notification to the police department.
- Warehouse doors are locked during normal business hours when warehouse personnel are unavailable.
- The reception area is staffed at all times during the working hours of 8:00 AM to 4:30 PM, Monday through Friday.
- Any unrecognized person in a restricted office location should be challenged as to their right to be there. All visitors must sign in at the front desk and be accompanied by a TW staff member. Visitors must indicate if they will be entering a secure area, show a government issued ID prior to entry and wear a visitor's badge.
- Swipe cards control access to our servers, data files and long-term storage. Each card is coded to allow admission to specific areas based on each individual's job function or need to know.
- The building is equipped with security cameras to record activities within the secure data area. All activities in these areas are recorded on a 24-hour a day 365 day per year basis.
- The secure data area is equipped with security alarms. If the door to the area is left open for an extended amount of time or opened by force an alarm will sound and 4 individuals identified by TW will be notified about the issue.
- Fire Protection: Use of local building codes will be observed. Manufacturer's recommendations on the fire protection of individual hardware will be followed.

Telecommuting

TW considers telecommuting to be an acceptable work arrangement in certain circumstances. This policy is applicable to all employees who work either permanently or only occasionally outside of the TW office environment. It applies to users who work from their home full time, to employees on temporary travel, to users who work from a remote office location, and to any user who connects to the TW network from a remote location.

GENERAL REQUIREMENTS

Telecommuting workers are required to follow all corporate, security, confidentiality, or Code of Conduct policies that are applicable to other employees/contractors.

Need to Know: Telecommuting Users will have the access based on the same 'need to know' as they have when in the office.
Password Use: The use of a strong password, changed at least every 60 days, is even more critical in the telecommuting environment. Do not share your password or write it down where a family member or visitor can see it.
Two-Factor Authentication: Users must authenticate using two methods prior to accessing the TW network.
Training: Personnel who telecommute must complete the same annual privacy training as all other employees.
Contract Specific: There may be additional requirements specific to the individual contracts to which an employee is assigned.

HARDWARE SECURITY PROTECTIONS

Virus/Malware Protection**:** Home users must never stop the update process for Virus/Malware Protection. Virus/Malware Protection software is installed on all TW computers and is set to update the virus pattern on a daily basis. This update is critical to the security of all data, and must be allowed to complete.

VPN**:** Established procedures must be rigidly followed when accessing TW information of any type. TW requires the use of VPN software. VPN access is granted upon approval from the Security Office and requires the use of dual authentication.

Lock Screens**:** No matter what location, always lock the screen before walking away from the workstation. The data on the screen may be protected by HIPAA or may contain confidential information. Be sure the automatic lock feature has been set to automatically turn on after 10 minutes of inactivity.

DATA SECURITY PROTECTION

Transferring Data to TW**:** Transferring of data to TW requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. Do not circumvent established procedures, nor create your own method, when transferring data to TW.

External System Access: If you require access to an external system, contact your supervisor or department head. Privacy Officer or appropriate personnel will assist in establishing a secure method of access to the external system.

E-mail: Do not send any individual-identifiable information (PHI or PII) via e-mail unless it is encrypted. If you need assistance with this, contact the Privacy Officer or appropriate personnel to ensure an approved encryption mechanism is used for transmission through e-mail.

Non-TW Networks: Extreme care must be taken when connecting TW equipment to a home or hotel network. Although TW actively monitors its security status and maintains organization wide protection policies to protect the data within all contracts, TW has no ability to monitor or control the security procedures on non-TW networks. TW requires that TW devices are only connected to password protected, secure networks.

Protect Data in Your Possession: View or access only the information that you have a need to see to complete your work assignment. Regularly review the data you have stored to ensure that the amount of patient level data is kept at a minimum and that old data is eliminated as soon as possible.

Hard Copy Reports or Work Papers: Never leave paper records around your work area. Lock all paper records in a file cabinet at night or when you leave your work area.

Data Entry When in a Public Location: Do not perform work tasks which require the use of sensitive corporate or patient level information when you are in a public area, i.e. airports, airplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind you.

MOBILE DEVICES

Any phone or mobile device that stores any data owned by TW, whether owned by TW or an individual staff member, must have the following security measures put in place:

- A screen lock must be implemented to require a password or code to be entered after being idle for 2 minutes or more.
- Staff members must not use the default passwords provided by their phone or voicemail service, but must create a new one.

No staff may add any data owned by TW to their personal phone or other device without the express permission of management. Data includes, but is not limited to, email, files, and database access through applications or web browsers.

In addition to the items outlined above, an individual who is given a phone owned by TW or granted permission to add data owned by TW on their phone or mobile device, agrees to the following:

- They will report any loss or theft of their phone or mobile device to management within 24 hours.
- They consent to having their phone's or mobile device's data wiped by our network support staff in the event of loss or theft to protect any data stored on the device.
- They agree to abide by best practices as outlined in this and other technology policies, which can be amended by management at any time.

Staff must receive written approval from their supervisor to utilize wi-fi provided by TW for their mobile device. If approval is granted, staff may only utilize guest wi-fi when connecting mobile devices.

Disposal of Paper & External Media/Hardware

DISPOSAL OF PAPER AND/OR EXTERNAL MEDIA

Shredding: All paper which contains sensitive information that is no longer needed must be shredded before being disposed. Do not place in a trash container without first shredding. It is acceptable to place materials to be shredded in the identified, locked shred bins. All employees working from home, or other non-TW work environment, MUST have direct access to a shredder.

Disposal of Electronic Media: All external media must be sanitized or destroyed in accordance with HIPAA compliant procedures.

- Do not throw any media containing sensitive, protected information in the trash.
- Return all external media to your supervisor
- External media must be wiped clean of all data.

Many state and federal laws regulate the retention and destruction of medical information. TW actively conforms to these laws and follows the strictest regulation if/when a conflict occurs.

Record Retention - Documents relating to uses and disclosures, authorization forms, business partner contracts, notices of information TW, responses to a patient who wants to amend or correct their information, the patient's statement of disagreement, and a complaint record are maintained for a period of 6 years.

Record Destruction - All hardcopy medical records that require destruction are shredded using NIST 800-88 guidelines.

Client Data – Client data not required to be kept for a certain duration by law will be destroyed upon the termination of a relationship between client and TotalWellness. An attestation of destruction will be provided to client upon request.

DISPOSAL OF EXTERNAL MEDIA

It must be assumed that any external media in the possession of an employee is likely to contain either protected health information (“PHI”) or other sensitive information. Accordingly, external media (CD-ROMs, DVDs, USB drives) should be disposed of in a method that ensures that there will be no loss of data and that the confidentiality and security of that data will not be compromised.

The following steps must be adhered to:

- It is the responsibility of each employee to identify media, which should be shredded, and to utilize this policy in its destruction.
- External media should never be thrown in the trash.
- When no longer needed all forms of external media are to be sent to the Privacy Officer or appropriate personnel for proper disposal.

- The media will be secured until appropriate destruction methods are used based on NIST 800-88 guidelines.
- Privacy Officer will notify DataShield when equipment is needed to be disposed of.

REQUIREMENTS REGARDING EQUIPMENT

All equipment to be disposed of will be wiped of all data, and all settings and configurations will be reset to factory defaults. No other settings, configurations, software installation or options will be made. Asset tags and any other identifying logos or markings will be removed.

DISPOSITION OF EXCESS EQUIPMENT

As the older TW computers and equipment are replaced with new systems, the older machines are held in inventory for a wide assortment of uses:

- Older machines are regularly utilized for spare parts.
- Older machines are used on an emergency replacement basis.
- Older machines are used for testing new software.
- Older machines are used as backups for other production equipment.
- Older machines are used when it is necessary to provide a second machine for personnel who travel on a regular basis.
- Older machines are used to provide a second machine for personnel who often work from home.

Contingency Plan

STATEMENT OF POLICY

To establish and implement policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, natural disaster) that damages systems that contain PHI.

TW is committed to maintaining formal procedures for responding to an emergency or other occurrence that damages systems containing PHI. TW shall continually assess potential risks and vulnerabilities to protect health information in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the HIPAA Security Rule.

PROCEDURE

1. Data Backup Plan

    a. TW, under the direction of the Security Officer, shall implement a data backup plan to create and maintain retrievable exact copies of PHI.

    b. At noon and at the conclusion of each day, Monday through Friday, an incremental backup of all servers containing ePHI shall be backed up.

    c. The Security Officer shall monitor storage and removal of backups and ensure all applicable access controls are enforced.

    d. All data is backed up based using best practices. A backup is completed on premises through a multifactor authenticated NAS. A backup copy is also stored through the cloud using Storagecraft's data cloud backup. All backups are encrypted in transit and at rest using the same standards as original data storage.

2. Disaster Recovery and Emergency Mode Operations Plan

    a. The Security Officer shall be responsible for developing and regularly updating the written disaster recovery and emergency mode operations plan for the purpose of:

        i. Restoring or recovering any loss of ePHI and/or systems necessary to make ePHI available in a timely manner caused by fire, vandalism, terrorism, system failure, or other emergency; and

        ii. Continuing operations during such time information systems are unavailable. Such written plan shall have a sufficient level of detail and explanation that a person unfamiliar with the system can implement the plan in case of an emergency or disaster.

b. The disaster recovery and emergency mode operation plan shall include the following:

    i. Current copies of the information systems inventory and network configuration developed and updated as part of TW's risk analysis.

    ii. Current copy of the written backup procedures developed and updated pursuant to this policy.

    iii. Identification of an emergency response team. Members of such team shall be responsible for the following:

        1. Determining the impact of a disaster and/or system unavailability on TW's operations.

        2. In the event of a disaster, securing the site and providing ongoing physical security.

        3. Retrieving lost data.

        4. Identifying and implementing appropriate "work-arounds" during such time information systems are unavailable.

        5. Taking such steps necessary to restore operations.

    iv. Procedures for responding to loss of electronic data including, but not limited to retrieval and loading of backup data or methods for recreating data should backup data be unavailable. The procedures should identify the order in which data is to be restored based on the criticality analysis performed as part of TW's risk analysis

    v. Telephone numbers and/or e-mail addresses for all persons to be contacted in the event of a disaster, including the following:

        1. Members of the immediate response team,

        2. Information systems vendors, and

        3. All current workforce members.

c. The disaster recovery team shall meet on at least an annual basis to:

    i. Review the effectiveness of the plan in responding to any disaster or emergency experienced by TW;

    ii. Review the written disaster recovery and emergency mode operations plan and make appropriate changes to the plan. The Security Officer shall be responsible for convening and maintaining minutes of such meetings. The Security Officer also shall be responsible for revising the plan based on the recommendations of the disaster recovery team.

Security Awareness and Training

STATEMENT OF POLICY

To establish a security awareness and training program for all members of TW's workforce, including management.

All workforce members shall receive appropriate training concerning TW's security policies and procedures. Such training shall be provided prior to the effective date of the HIPAA Security Rule and on an ongoing basis to all new employees. Such training shall be repeated annually for all employees.

PROCEDURE

a. Security Training Program

   i. The Security Officer shall have responsibility for the development and delivery of initial security training. All workforce members shall receive such initial training addressing the requirements of HIPAA. Security training shall be provided to all new workforce members as part of the orientation process. Attendance and/or participation in such training shall be mandatory for all workforce members. The Security Officer shall be responsible for maintaining appropriate documentation of all training activities.

   ii. The Security Officer shall have responsibility for the development and delivery of ongoing security training provided to workforce members in response to environmental and operational changes impacting the security of ePHI, e.g., addition of new hardware or software, and increased threats.

b. Security Reminders

   i. The Security Officer shall generate and distribute to all workforce members routine security reminders on a regular basis. Periodic reminders shall address password security, malicious software, incident identification and response, and access control. The Security Officer may provide such reminders through formal training, e-mail messages, discussions during staff meetings, newsletter/intranet articles, and posters. The Security Officer shall be responsible for maintaining appropriate documentation of all periodic security reminders.

   ii. The Security Officer shall generate and distribute special notices to all workforce members providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures.

c. Protection from Malicious Software

   i. As part of the aforementioned Security Training Program and Security Reminders, the Security Officer shall provide training concerning the prevention, detection, containment, and eradication of malicious software. Such training shall include the following:

a) Guidance on opening suspicious e-mail attachments, e-mail from unfamiliar senders, and hoax e-mail,

b) The importance of updating anti-virus software and how to check a workstation or other device to determine if virus protection is current,

c) Instructions to never download files from unknown or suspicious sources,

d) Recognizing signs of a potential virus that could sneak past antivirus software or could arrive prior to an update to anti-virus software,

e) The importance of backing up critical data on a regular basis and storing the data in a safe place,

f) Damage caused by viruses and worms, and

g) What to do if a virus or worm is detected.

d. Password Management

i. As part of the aforementioned Security Training Program and Security Reminders, the Security Officer shall provide training concerning password management. Such training shall address the importance of confidential passwords in maintaining computer security, as well as the following requirements relating to passwords:

a) Passwords must be changed every 60 days.

b) Passwords must be at least eight characters and contain upper case letters, lower case letters, numbers, and special characters.

c) Commonly used words, names, initials, birthdays, or phone numbers should not be used as passwords.

d) A password must be promptly changed if it is suspected of being disclosed or known to have been disclosed.

e) Passwords must not be disclosed to other workforce members (including anyone claiming to need a password to “fix” a computer or handle an emergency situation) or individuals, including family members.

f) Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.

g) Employees should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.

h) Any employee who is directed by the Security Officer to change his/her password to conform to the aforementioned standards shall do so immediately.

Security Management Process

STATEMENT OF POLICY

To ensure TW conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by TW.

TW shall conduct an accurate and thorough risk analysis to serve as the basis for TW's HIPAA Security Rule compliance efforts. TW shall re-assess the security risks to its ePHI and evaluate the effectiveness of its security measures and safeguards as necessary in light of changes to business TWs and technological advancements.

PROCEDURE

a. The Security Officer shall be responsible for coordinating TW's risk analysis. The Security Officer shall identify appropriate persons within the organization to assist with the risk analysis.

b. The risk analysis shall proceed in the following manner:

    i. Document TW's current information systems.

        a) Update/develop information systems inventory.

        b) Update/develop facility layout showing location of all information systems equipment, power sources, telephone jacks, and other telecommunications equipment, network access points, fire and burglary alarm equipment, and storage for hazardous materials.

        c) For each application identified, identify each licensee (*i.e.,* authorized user) by job title and describe the manner in which authorization is granted.

        d) For each application identified:

            i) Describe the data associated with that application.

            ii) Determine whether the data is created by the organization or received from a third party. If data is received from a third party, identify that party and the purpose and manner of receipt.

            iii) Determine whether the data is maintained within the organization only or transmitted to third parties. If data is transmitted to a third party, identify that party and the purpose and manner of transmission.

            iv) Define the criticality of the application and related data as high, medium, or low. Criticality is the degree of impact on the organization if the application and/or related data were unavailable for a period of time.

v) Define the sensitivity of the data as high, medium, or low. Sensitivity is the nature of the data and the harm that could result from a breach of confidentiality or security incident.

vi) For each application identified, identify the various security controls currently in place and locate any written policies and procedures relating to such controls.

e) Identify and document threats to the confidentiality, integrity, and availability (referred to as "threat agents") of ePHI created, received, maintained, or transmitted by TW. Consider the following:

i) Natural threats, e.g., earthquakes, storm damage.

ii) Environmental threats, e.g., fire and smoke damage, power outage, utility problems.

iii) Human threats

a. Accidental acts, e.g., input errors and omissions, faulty application programming or processing procedures, failure to update/upgrade software/security devices, lack of adequate financial and human resources to support necessary security controls

b. Inappropriate activities, e.g., inappropriate conduct, abuse of privileges or rights, workplace violence, waste of corporate assets, harassment

c. Illegal operations and intentional attacks, e.g., eavesdropping, snooping, fraud, theft, vandalism, sabotage, blackmail

d. External attacks, e.g., malicious cracking, scanning, demon dialing, virus introduction

iv) Identify and document vulnerabilities in TW's information systems. A vulnerability is a flaw or weakness in security policies and procedures, design, implementation, or controls that could be accidentally triggered or intentionally exploited, resulting in unauthorized access to ePHI, modification of ePHI, denial of service, or repudiation (*i.e.,* the inability to identify the source and hold some person accountable for an action). To accomplish this task, conduct a self-analysis utilizing the standards and implementation specifications to identify vulnerabilities.

f) Determine and document probability and criticality of identified risks.

i) Assign probability level, i.e., likelihood of a security incident involving identified risk.

a. "Very Likely" (3) is defined as having a probable chance of occurrence.

b. "Likely" (2) is defined as having a significant chance of occurrence.

c. "Not Likely" (1) is defined as a modest or insignificant chance of occurrence.

ii) Assign criticality level.

a. "High" (3) is defined as having a catastrophic impact on the medical TW including a significant number of medical records which may have been lost or compromised.

b. "Medium" (2) is defined as having a significant impact including a moderate number of medical records within TW which may have been lost or compromised.

c. "Low" (1) is defined as a modest or insignificant impact including the loss or compromise of some medical records.

iii) Determine risk score for each identified risk. Multiply the probability score and criticality score. Those risks with a higher risk score require more immediate attention.

g) Identify and document appropriate security measures and safeguards to address key vulnerabilities. To accomplish this task, review the vulnerabilities you have identified in relation to the standards and implementation specifications. Focus on those vulnerabilities with high risk scores, as well as specific security measures and safeguards required by the Security Rule.

h) Develop and document an implementation strategy for critical security measures and safeguards.

i) Determine timeline for implementation.

ii) Determine costs of such measures and safeguards and secure funding.

iii) Assign responsibility for implementing specific measures and safeguards to appropriate person(s).

iv) Make necessary adjustments based on implementation experiences.

v) Document actual completion dates.

i. Evaluate effectiveness of measures and safeguards following implementation and make appropriate adjustments.

c. The Security Officer shall be responsible for identifying appropriate times to conduct follow-up evaluations and coordinating such evaluations. The Security Officer shall identify appropriate persons within the organization to assist with such evaluations. Such evaluations shall be conducted upon the occurrence of one or more of the following events: changes in the HIPAA Security Regulations; new federal, state, or local laws or regulations affecting the security of ePHI; changes in technology, environmental processes, or business processes that may

affect HIPAA Security policies or procedures; or the occurrence of a serious security incident. Follow-up evaluations shall include the following:

i. Inspections, reviews, interviews, and analysis to assess adequacy of administrative and physical safeguards. Such evaluation shall include interviews to assess employee compliance; after-hours walk-through inspections to assess physical security, password protection (i.e., not posted), and workstation sessions terminated (i.e., employees logged out); review of latest security policies and procedures for correctness and completeness; and inspection and analysis of training, incident, and media logs for compliance.

ii. Analysis to assess adequacy of controls within the network, operating systems and applications. As appropriate, TW shall engage outside vendors to evaluate existing physical and technical security measures and make recommendations for improvement