INFORMATION TECHNOLOGY SECURITY

POLICY AND PROCEDURES MANUAL

By

Waymakers
1221 East Dyer Road, Suite 120
Santa Ana, CA 92705
(949) 250-0488

MARCH 2018

TABLE OF CONTENTS

HIPAA

This overview of Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Standards is based on Waymakers' review of 45 CFR 164. These Standards have been enacted by the Department of Health and Human Services to give the health care industry a minimum set of administrative, technical and physical safeguards to protect the confidentiality, integrity and availability of Protected Health Information.

PROTECTED HEALTH INFORMATION

As defined in HIPAA, Protected Health Information (PHI) is a type of individually identifiable health information that is maintained or transmitted in any medium and that provides information about:

1) an individual's past, present, or future physical and mental health condition;
2) the provision of health care to the individual; or
3) Past, present, or future payment for health care provided to the individual.

REMOVAL OF 18 TYPES OF PHI IDENTIFIERS

Section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of protected health information. Under this standard, health information is not individually identifiable if it does not identify an individual and if the covered entity has no reasonable basis to believe it can be used to identify an individual. To de-identify information, you must remove the following 18 types of PHI Identifiers:

1. Names;
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Phone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social Security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;

13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)

There are also additional standards and criteria to protect individual's privacy from re-identification. Any code used to replace the identifiers in datasets cannot be derived from any information related to the individual and the master codes, nor can the method to derive the codes be disclosed. For example, **a client's initials cannot be used to code their data** because the initials are derived from their name. In other words, the information would still be considered identifiable is there was a way to identify the individual even though all of the 18 identifiers were removed.

AUTHORIZATION TO DISCLOSE

Documents requested to be shared between parties need to have a signed Authorization to Disclose (ATD) form accompany the document. The ATD and document(s) should be faxed over a secure line with a confidentiality statement and a follow-up call made to the recipient to verify receipt of the ATD and document(s) to the appropriate party. Revocation of the ATD can occur anytime at the written request of the consumer. Unless otherwise revoked in writing by the consumer the authorization expires upon discharge from the program.

MINIMUM NECESSARY STANDARD

[*45 CFR 164.502(b), 164.514(d)*]

The minimum necessary standard, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information. The Privacy Rule's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity.

ADMINISTRATIVE SAFEGUARDS

Administrative Safeguards are defined in the Security Rule as the "administrative actions and policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."

There are eight security standards:

1. **Security management process**. This standard has four implementation specifications to prevent, detect, punish, and correct security violations:

a. **Risk Analysis.** WAYMAKERS has subcontracted for Information Technology services from [redacted].and [redacted] has conducted an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of Electronic Private Health Information (EPHI) held by WAYMAKERS and WAYMAKERS has implemented cost-effective security measures to guard against inadvertent or unauthorized uses or disclosures of EPHI.

Computer, Software, Network, and Internet Risk Assessment

Risk analysis is the process of identifying what you need to protect, what you need to protect it from, and how to protect it. Evaluate the network to determine which assets are worth protecting and the extent to which these assets should be protected. In principle, the cost of protecting a particular asset should not be more than the asset itself. A detailed list of all assets will include both tangible objects, such as servers and workstations, and intangible objects, such as software and data.
Once the assets requiring protection are identified, it is necessary to identify the threats to these assets. The threats can then be examined to determine what potential for loss exists.

WAYMAKERS Tangible Assets

- Servers, network attached storage, routers and switches
- Workstations
- Mobile computers (Laptops)

WAYMAKERS Software and Data

- 3rd Party Software: Examples: Accufund, Caminar, Mad Trac Restitution, PGP, Acrobat Pro, Illustrator, Photoshop
- Server Operating System software, workstation operating software, Office productivity software
- Company Public data: data that is intended for the general use of the company personnel
- Company Confidential Data: Data protected by the Privacy Act, HIPAA or other regulatory statutes.

Threats to company assets are considered low. The most valuable asset to WAYMAKERS is the data that is created in the general course of business. The principle source of a threat is from company personnel and either abuse or misuse of data, malicious acts or inadvertent disclosure of private information. Physical security is sufficient with regard to company access controls. Possible disaster such as fire or flood is also present.

b. **Risk Management.** WAYMAKERS has implemented security measures to reduce risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by the WAYMAKERS.

Computer, Software, Network, and Internet Policy with Appropriateness of Use Guidelines

Approval Authority:
Issued under the authority of the Executive Director of WAYMAKERS

Application:
Personnel of WAYMAKERS to include full-time, part-time, relief, office, intern, and student personnel

Policy statement:
WAYMAKERS sponsored computer and or network connections shall be used only by authorized users, for legitimate WAYMAKERS business related purposes.

Policy requirements:
This policy concerns all use of computers, and connections to the company network and the Internet made on behalf of WAYMAKERS. The use of WAYMAKERS computers and company network and Internet connections and facilities (referred to herein as The WAYMAKERS Network) are for official WAYMAKERS uses only. Use of the WAYMAKERS computers and company network and Internet connections and facilities is restricted to activities that legitimately further the operations and programs of WAYMAKERS.

Supervision of users:
The Management of WAYMAKERS should be aware of their subordinates' WAYMAKERS Network usage. Managerial accountability for the actions of subordinates applies equally to The WAYMAKERS Network use as to any other activity. The WAYMAKERS Network consists of all facilities used by WAYMAKERS to connect to the local area network (LAN), the wide area network (WAN), and the global Internet.

Privacy and monitoring:
There is no guarantee of privacy in using The WAYMAKERS Network, including e-mail communication. WAYMAKERS reserves the right to monitor all user WAYMAKERS Network communications and examine all information collected, created and/or generated as a result of using The WAYMAKERS Network including any files, messages, printouts, removable media, or other material in order to monitor users' compliance with this policy.

Ethics:
All users shall behave in a proper, ethical, and legal manner consistent with WAYMAKERS standards when they use The WAYMAKERS Network as they are entering into a public forum and any actions taken will reflect on WAYMAKERS as a whole.

c. **Sanction Policy.** WAYMAKERS has a disciplinary process to apply appropriate sanctions against workforce members who fail to comply with WAYMAKERS' Information Technology Security Policy. WAYMAKERS will discipline employees for violating the security policies and

procedures. Such discipline could include written warnings or terminating employees for egregious violations.

d. **Information System Activity Review.** The designated Privacy Officer and Security Officer will work together to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports to determine if any EPHI is being used or disclosed inappropriately.

2. **Assigned security responsibility.**

a. WAYMAKERS has designated Hether Benjamin as the Privacy Officer for the Agency to obtain advice regarding privacy issues surrounding the disposition of PHI and the media upon which it may be recorded. WAYMAKERS has designated [redacted] a subcontractor for WAYMAKERS, Inc., as the Security Officer to manage the security of its information surrounding the disposition of EPHI and the media upon which it may be recorded.

3. **Workforce security.** The Security Officer will implement security measures to all employees who need to have access to EPHI the access that they need to perform their work activities and that employees who do not need to have access to EPHI do not have such access.

a. **Authorization and Supervision.** Human Resources will provide authorization to the Security Officer of workforce members who work with EPHI to grant or revoke access to EPHI. Authorization, which means the act of determining whether a particular person has the right to carry out a particular function, and the concomitant subject of authentication, which means having a particular user prove that he or she is such user by using passwords to verify credentials.

b. **Workforce Clearance Procedure**. To help ensure that individuals joining WAYMAKERS are well qualified and have the potential to be productive and successful, WAYMAKERS checks the employment history and references of employment candidates. Job offers will be extended contingent upon the satisfactory completion of all reference and background checks. Human Resources will conduct personnel and professional reference checks before allowing anyone to access EPHI.

c. **Termination Procedures.** Employees are required to return all WAYMAKERS property in their possession or control immediately on termination of employment for any reason. When the employment of a workforce member ends, Human Resources will provide authorization to the Security Officer to implement security steps to follow when an employee is terminated, such as changing passwords, removing the employee from access lists, deleting profiles, wiping hard drives clean, etc.

4. **Information access management**. The Security Officer will implement, monitor, manage and/or revoke access to information technology used by WAYMAKERS.

a. **Isolating Health Care Clearinghouse Functions**. This specification is not applicable to WAYMAKERS.

b. **Access Authorization.** Upon authorization from Human Resources for new employees or the Program Director for existing employees, the Security Officer will grant access to EPHI for a particular program employee, for example, through access to a workstation, transaction, program, or process. The Security Office will grant and maintain privileges for individuals to access EPHI. The Security Officer will keep access authorization records that document the access to EPHI that each employee has, including why such employee has such access.

c. **Access Establishment & Modification.** The Security Officer will implement access authorization, establish, document, review, and modify a user's right of access to a workstation, program, or process, review these issues on an ongoing basis and document any changes.

5. **Security awareness and training.** All workforce members with access to EPHI will complete a compliance training addressing WAYMAKERS' Information Technology Security Policy.

a. **Security Reminders.** WAYMAKERS will conduct annual reviews of its Information Technology Security Policy to determine if they need to be updated and will annually remind employees of their security responsibilities or provide updates as needed.

b. **Protection from Malicious Software**. To guard against malicious software, WAYMAKERS does not allow anyone to bring in any software or diskettes from home or allow anyone to download any games, data, or software that have not been authorized or checked by the Security Officer. WAYMAKERS has virus protection software in place to detect computer viruses.

c. **Log-in Monitoring.** Log-in attempts are monitored. Users are allowed five (5) log-in attempts. After five (5) failed attempts the user account is locked and access is denied.

d. **Password Management.** The Security Officer will implement network security (see "Technical Safeguards" policy) rules that require users to create and change passwords according to policy guidelines. Users will be required to follow the password policy pertaining to safeguarding passwords and the proper use of strong passwords. (Note: passwords are proprietary and the Security Officer does not create, change, or safeguard user passwords)

6. **Security incident procedures.** The Security Officer will respond to known security incidents and report incidents to Human Resources and the Privacy Officer. A security incident is defined as an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

a. **Response & Reporting.** The Security Officer will identify, respond to, and document suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known; and document their outcome to report to Human Resources and the Privacy Officer.

7. **Contingency plan**. The Security Officer will respond as soon as possible but within 24 hours to an emergency or other occurrence that damages WAYMAKERS' equipment or systems containing EPHI. The Security Officer will determine:

- The type of emergency

- Who should be contacted and what the priority will be. (Police, fire company officers etc.)
- Preliminary damage and risk assessment
- Temporary course of action to secure the company assets until company administrators can be informed and make further decisions

a. **Data Backup Plan**. All user created data is backed up on a daily basis. Backups are maintained on designated secure servers or NAS devices. Backup Data Access is subject to user authentication and password protected. User access is limited to authorized persons as determined by WAYMAKERS administration.

b. **Disaster Recovery Plan.** In the event of a disaster, the following actions will be taken by the Security Officer to restore any loss of data:

- Assess the extent of the damage.
- Determine what recovery actions are needed (i.e. temporary facilities, hardware replacement of infrastructure and equipment, software replacement and data recovery).
- The priority of recovery actions.
- Report to the administration.
- Execute recovery procedures upon approval.

c. **Emergency Mode Operation Plan**. To enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode, the Security Officer will prepare a report to the administration after the initial first response to an emergency. The report will contain information directly related to hardware, software and electronic data stored and maintained by the company. The Security Officer will follow the priority determined by the administration to restore hardware and software and access to EPHI on a temporary basis.

d. **Testing & Revision Procedures.** From time to time as determined by the company administration, the Security Officer will review the contingency plan for relevance with respect to the current network infrastructure, installed hardware and software, and data recording and storage. The Security Officer may suggest improvements or additions in areas that have been affected by advances in technology that may afford greater flexibility, security, economy and effectiveness in the event the company is obliged to operate in Contingency Mode.

e. **Applications & Data Criticality Analysis**. Applications and Data Criticality is determined by the priority of then current activities engaged in by WAYMAKERS. By default, hardware, operating system software and network connectivity must be restored. Office productivity software must also be restored as a first priority. Certain 3rd party applications are considered critical to the operations of the company, but, the order of priority required at a given point in time will be relative to the immediate needs of the company at that specific time and will be determined by the company administrators.

8. **Evaluation.** The Privacy Officer will perform a periodic non-technical evaluation to determine the extent to which WAYMAKERS' Information Technology Security Policy meets the requirements of the HIPAA security regulations. The Security Officer will perform a periodic technical evaluation to determine the extent to which the WAYMAKERS's Information Technology Security Policy meets the requirements of the security regulations.

a. **Business Associate Contracts.** WAYMAKERS does not currently permit a business associate to create, receive, maintain, or transmit EPHI on behalf of WAYMAKERS.

PHYSICAL SAFEGUARDS

Physical Safeguards - are defined as the "physical measures, policies, and procedures to protect WAYMAKERS' electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."

There are four physical safeguards:

1. **Facility access controls**. The computer/server room within the facility is locked to limit physical access to electronic information systems and access is provided to individuals authorized by the Security Officer only.

a. **Contingency Operations**. The Security Officer or Privacy Officer will allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency, to ensure that those who need access to EPHI, in the event of an emergency, are able to get such access.

b. **Facility Security Plan.** WAYMAKERS' corporate facility is secured with locking entry doors and monitored by a security company to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. Additional precautions include locks on office doors, issuing keys to certain authorized individuals, and locating workforce members in places where they can see and control what is going on in the practice.

c. **Access Control & Validation Procedures.** Human Resources will coordinate with the Security Officer to validate a workforce member's access to facilities based on his or her role or function, including visitor control, and control of access to software programs for testing and revision, in order to limit physical access to its facilities to only appropriately authorized individuals.

d. **Maintenance Records.** The Director of Finance and Administration will execute and document repairs and modifications to the physical components of its facility that are related to security.

2. **Workstation use.** WAYMAKERS' Worksite Equipment Usage policy is outlined in the Employee Handbook and describes what tasks can be performed at a particular workstation, how those tasks are to be performed, and the physical surroundings of workstations. In addition, WAYMAKERS requires workforce members who access EPHI to ensure that casual observers

cannot view computer screens with EPHI on them by physically arranging the location of their screen or attaching a security screen to the monitor.

3**. Workstation security**. WAYMAKERS locates workstations in secure areas whenever possible. However, the WAYMAKERS also limits physical access to computers by utilizing access controls, passwords, locks on doors, and automatic logoffs.

4. **Device & media controls.** EPHI will not be permanently stored on agency issued mobile equipment. EPHI will not be stored on removable media devices. Users must password-protect any consumer sensitive data used in the field. Any data temporarily saved on a mobile hard drive while in the field will be transferred to the secure server upon return to the facility. Laptops will be powered down after use whenever in the field. Removable media devices (i.e., USB's, CD's., DVD's, etc.) are not authorized for u se with the transmittal or storage of EPHI.

a. **Disposal.** Before disposal of any hardware or electronic media used in connection with EPHI, the data is removed by the use of software that "wipes" or scrubs (also known as a Data Dump) all data through the use of disk wiping algorithms.

b. **Media Re-use**. The Security Officer will overwrite the storage space on the hard drive when equipment is transferred between workforce members to ensure the removal of EPHI from electronic media before the media are made available for re-use.

c. **Accountability.** The Director of Finance and Administration maintains a record of the hardware and electronic media and any person responsible by program through an up -to- date inventory of any hardware and related mobile devices or media that contain EPHI.

d. **Data Backup & Storage.** The Security Officer will implement a back-up process to create a retrievable, exact copy of EPHI, when needed, before the equipment is moved.

TECHNICAL SAFEGUARDS

Technical Safeguards - are defined as the "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

There are five technical safeguards:

1. Access control. The Security Officer will assign access rights only to those workforce members who require this for their job role as authorized by Human Resources. The Security Officer will maintain administrative rights.

a. Unique User Identification. The Security Officer assigns a unique user name for identifying and tracking user identity, access levels and a temporary password. The workforce member is tasked with changing the temporary password and instructed to make the password strong to make them difficult to decode or guess. The workforce member is instructed to not share this password with anyone.

b. Emergency Access Procedure. The Security Officer will be responsible for obtaining necessary EPHI during an emergency.

c. Automatic Log-off. Computers that have access to EPHI are configured to activate the computer lock feature after a designated time period of inactivity. The user must enter password credentials to unlock the computer.

d. Encryption & Decryption. All data transmission over an "open" network like the internet that the company engages in is specifically, e-mail, email attachments, and through a VPN. The VPN connections are secure and encrypted during transmission from point to point. Files or attachments to e-mail messages are encrypted before they are transmitted. WAYMAKERS does not allow transmission of EPHI in the body of any e-mail messages. Agency issued laptops which transmit or store EPHI are required to have a pre-boot authentication using a strong password and full disk encryption.

2. Audit controls. Certain events are audited on the WAYMAKERS Network in order to enhance security and provide information in the event of unwarranted activity. WAYMAKERS Network Audit controls are as follows:

- Logon events: Audits attempts to log on to workstations and member servers.
- Object Access: Audits attempts to access an object such as a file or folder.
- Policy change: Audits any change to user rights assignments, audit, account, or trust policies.

3. Integrity. WAYMAKERS workforce members are required to protect EPHI from being improperly changed or destroyed during the course of their day to day duties and should not be altered without the WAYMAKERS Program Director's knowledge or approval.

4. Person or entity authentication. The Security Officer will coordinate with Human Resources to verify that a workforce member seeking access to EPHI is who they claim to be and are authorized per their job role to have such access.

5. Transmission security. WAYMAKERS will implement the following security measures in an effort to prevent unauthorized access to EPHI that is being transmitted over an electronic communications network:

a. Integrity Controls. WAYMAKERS workforce members are required to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed during the course of their day to day duties and should not be altered without the WAYMAKERS Program Director's knowledge or approval.

b. Encryption. WAYMAKERS encrypts all EPHI that is transmitted through the company VPN, or contained in an e-mail attachment. Laptop computers used to create EPHI use whole disk encryption and are not used to permanently store data.